NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CYBERSECURITY: UTILIZING FUSION CENTERS TO PROTECT STATE, LOCAL, TRIBAL, AND TERRITORIAL ENTITIES AGAINST CYBER THREATS

by

Payton A. Flynn, Sr.

September 2016

Thesis Advisor: John Rollins
Second Reader: Lauren Fernandez

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2016	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE CYBERSECURITY: UTILIZING FUSION CENTERS TO PROTECT STATE, LOCAL, TRIBAL, AND TERRITORIAL ENTITIES AGAINST CYBER THREATS			**5. FUNDING NUMBERS**
6. AUTHOR(S) Payton A. Flynn, Sr.			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

Many areas of the cyber domain of American citizens are under attack: critical infrastructure, electrical grids, banks, businesses, government, and personally identifiable information (identity theft, medical records, child exploitation, etc.). Although the focus of recent cybersecurity legislation has provided additional authorities to federal agencies, a key concern for state, local, tribal and territorial (SLTT) government entities is this: What is the best way to protect computer networks at the state and local level? State and local governments have the responsibility to protect dams, freeway systems, power and water plants, emergency communications, personal identifiable information, health care records, educational institutions, and banking systems. The array of responsibilities and the cybersecurity threat landscape make state- and local-level computer networks fertile ground for the cyber adversary. This research focuses on the threat to SLTT computer networks and how to leverage information-sharing initiatives, cybersecurity policies and state and local fusion centers to prevent, mitigate, and deter cyber threats targeted at SLTT computer networks.

14. SUBJECT TERMS cybersecurity, cyber security, DHS, fusion, fusion center, information sharing, intelligence, NCCIC, NSA, NTOC, team, cyber threat, cyber mission			**15. NUMBER OF PAGES** 119
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

CYBERSECURITY: UTILIZING FUSION CENTERS TO PROTECT STATE, LOCAL, TRIBAL, AND TERRITORIAL ENTITIES AGAINST CYBER THREATS

Payton A. Flynn, Sr.
DHS/NCCIC Liaison Officer to NSA/NTOC,
Department of Homeland Security, Washington, D.C.
B.S., Capital University, 1991
M.S., National Intelligence University, 1996

MASTER OF ARTS IN SECURITY STUDIES (HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
September 2016

Approved by: John Rollins
Thesis Advisor

Lauren Fernandez
Second Reader

Erik Dahl
Associate Chair of Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Many areas of the cyber domain of American citizens are under attack: critical infrastructure, electrical grids, banks, businesses, government, and personally identifiable information (identity theft, medical records, child exploitation, etc.). Although the focus of recent cybersecurity legislation has provided additional authorities to federal agencies, a key concern for state, local, tribal and territorial (SLTT) government entities is this: What is the best way to protect computer networks at the state and local level? State and local governments have the responsibility to protect dams, freeway systems, power and water plants, emergency communications, personal identifiable information, health care records, educational institutions, and banking systems. The array of responsibilities and the cybersecurity threat landscape make state- and local-level computer networks fertile ground for the cyber adversary. This research focuses on the threat to SLTT computer networks and how to leverage information-sharing initiatives, cybersecurity policies and state and local fusion centers to prevent, mitigate, and deter cyber threats targeted at SLTT computer networks.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

#GOP	Guardians of Peace
ACS	Automated Case Support
CAE	Centers of Academic Excellence
CCIC	Cyber Intrusion Command Center
CCNIRT	Cyber and Computer Network Incident Response Team
CDEST	Cybersecurity Defensive Engagement Support Teams
CIA	Central Intelligence Agency
CIKR	critical infrastructure and key resources
CIO	Chief Information Officer
CIPAC	Critical Infrastructure Partnership Advisory Council
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CNA	computer network attack
CNCI	Comprehensive National Cybersecurity Initiative
CPLAP	Cybersecurity Partner Local Access Plan
CRR	cyber resilience review
CRS	Congressional Research Service
CS&C	cybersecurity and communications
CSA	Cyber Security Advisor Program
CSEP	Cyber Security Evaluation Program
CSG	combat support group
D/A	departments and agencies
DDoS	distributed denial of service attacks
DHS	Department of Homeland Security
DIB	defense industrial base
DNI	Director of National Intelligence
DNS	domain name system
DOD	Department of Defense
DOJ	Department of Justice
ECS	Enhanced Cybersecurity Service
EO	executive order
EOC	emergency operations center
FBI	Federal Bureau of Investigation
FCLP	Fusion Center Leaders Program
FEMA	Federal Emergency Management Agency
GAO	Government Accounting Office

HSAC	Homeland Security Advisory Council
HSDN	Homeland Secure Data Network
HSPD-7	Homeland Security Directive 7
IA	Information Assurance
IACP	International Association of Chiefs of Police
IAE	Information Assurance Education
ICS	industrial control systems
ICS-CERT	Industrial Control Systems-CERT
IM	instant messaging
ISAC	Information Sharing and Analysis Center
ISAO	information sharing and analysis organization
ISE	Interagency Sharing Environment
IT	Information technology
ITACG	Interagency Threat Assessment and Coordination Group
IT-GCC	IT-Government Coordinating Council
IT-SCC	Information Technology Sector Coordination Council
JTTF	Joint Terrorism Task Force
JWICS	Joint Worldwide Intelligence Communications System
LAPD	Los Angeles Police Department
LA-SAFE	Louisiana State Analytical and Fusion Exchange
MBR	master boot record
MCAC	Maryland Fusion Center
MIC3	Michigan Cyber Civilian Corps
MOA	memorandum of agreement
MS-ISAC	Multi-State Information Sharing and Analysis Center
NCCIC	National Cybersecurity and Communications Integration Center
NCRIC	Northern California Regional Center
NFCA	National Fusion Center Association
NGA	National Governors Association
NPPD	National Protection and Programs Directorate
NPR	National Preparedness Report
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OPM	Office of Personnel Management
PBS	Public Broadcasting Service
PII	personal identifiable information
PPD	Presidential Policy Directive
PSA	protective security advisor

ROI	return on investment
SA	security advisor
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facilities
SCION	SCI Operational Network
SECIR	strategic engagement and cyber infrastructure resilience
SIGINT	signals intelligence
SLTT	state, local, tribal and territorial
SOC	security operations center
SSL	secure socket layer
TTPs	tactics, techniques, and procedures
USCC	U.S. Cyber Command
US-CERT	United States Computer Emergency Readiness Team
VPN	virtual private network

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Many areas of the cyber domain are under attack: critical infrastructure, electrical grids, banks, business, government, and the personally identifiable information (identity theft, medical records, child exploitation, etc.) of American citizens. Although the focus of recent cybersecurity legislation has provided additional authorities to federal agencies, a key concern for state, local, tribal and territorial (SLTT) government entities is this: What is the best way to protect computer networks at the state and local level? This research focuses on the threat to SLTT computer networks and how to leverage information-sharing initiatives, cybersecurity policies and state and local fusion centers to prevent, mitigate, and deter cyber threats targeted at SLTT computer networks.

The reliance on computers within our society will continue to increase while new and increasingly sophisticated types of internet-connected devices will continue to be relied upon for life-sustaining activities that support most aspects of modern society. The lack of a collaborative strategy and framework at the state and local level to address the problem places SLTT entities and critical infrastructure networks at an increased risk of compromise.

The cyber threat to America's critical infrastructure, government networks, electrical grids, finance, education, military, and its citizens is not new. The threat happens daily, and it appears it will continue on into the future. The cyber threat happens under the cloak of secrecy. The adversaries are able to hide their identity while stealing intellectual property, financial information, or personal identifiable information. The combined threat posed by software vulnerabilities, nation-state actors, criminals, and hacktivist provide an increasingly tough challenge to U.S. cyber defenders. The threat is compounded by weaknesses in computer networks that render federal and critical infrastructure systems vulnerable to cyber attacks. The need for comprehensive approach to cybersecurity at all levels of government is needed to deter the threat.

A 2015 cybersecurity study "State of Cybersecurity in Local, State, and Federal Government," conducted by the Ponemon Institute, identified 86 percent of respondents

in state and local government who believe the responsibility for managing cybersecurity risk in their organizations is the most stressful job they have.[1] The Ponemon report points to the need for a more focused approach at the cybersecurity level. The approach should be scalable with the ability to share information efficiently from state to state. The information within the report identifies the need for an increased emphasis on ensuring state and local entities develop a cybersecurity mission and implement strategies and policies designed to prevent, mitigate, and deter cyber threats targeted at state and local government computer networks.

This thesis examines the implementation of policies, strategies, operational principles, and frameworks to address the cybersecurity protection needs of SLTT entities. The study focuses on regional state and local fusion centers to absorb a cyber mission. The fusion centers inherent mission is to "correlate the gathering, analysis, correlation, and sharing of threat related information between the federal government and SLTT organizations."[2] The research also examines authorities and reviews whether state and local fusion centers could be used as a mechanism to prevent, protect, mitigate, and recover from cyber attacks at the state and local levels.

[1] "The State of Cybersecurity in Local State and Federal Governments," accessed December 3, 2015, http://ponemon.org/blog/the-state-of-cybersecurity-in-local-state-and-federal-government.

[2] "State and Major Urban Area Fusion Centers," accessed February 11, 2014, http://www.dhs.gov/state-and-major-urban-area-fusion-centers.

ACKNOWLEDGMENTS

I first give all honor and glory to God from whom all blessings flow. I thank Him for the wisdom, knowledge, courage, and strength in making this experience and project such a wonderful blessing.

I thank my wife, Naomi, and our children, Payton and Simone, for their love, support, and encouragement during the program and my extended thesis journey. Their support during this project is truly a blessing and could not have been accomplished without them. I love you all so very much.

I thank my thesis advisors, Mr. John Rollins, and Dr. Lauren Fernandez, for their unending support during this long thesis project. I am truly grateful for your encouragement. I would also like to thank the Center for Homeland Defense and Security professors, administrators, and staff for the best graduate-level homeland security leadership education in the country. Your experience, dedication, encouragement, and support are exemplary.

Lastly, I would like to thank my friends and classmates in Cohort 1205/1206. I am still in awe of the contributions each of you makes to U.S. national security and the homeland security enterprise in particular. Your professionalism, dedication, and love for what you do are truly inspiring. A special thanks to Team Awesome. You are the best, and I will always cherish our friendship.

In closing, President Barack Obama once said, “If you’re walking down the right path and you’re willing to keep walking, eventually you’ll make progress.”

I thank God for progress.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> The cyber threat is one of the most serious economic and national security challenges we face as a nation … America's economic prosperity in the 21st century will depend on cybersecurity.
>
> ~ The White House

A. PROBLEM SPACE

Many areas of the cyber domain of American citizens are under attack: critical infrastructure, electrical grids, banks, business, government, and the personally identifiable information (identity theft, medical records, credit card information, etc.). The focus of Presidential Policy Directive (PPD)-21 is to "strengthen and maintain a secure and resilient critical infrastructure."[1] The policy calls for a "shared responsibility between the Federal departments/agencies, State, Local, Tribal and Territorial (SLTT) entities, and public and private owners and operators of critical infrastructure."[2] The threats to state and local governments can be directly related to homeland security cyber vulnerabilities. This thesis focuses on the threat to SLTT computer networks and how to leverage information sharing initiatives, cybersecurity policies and state and local fusion centers to prevent, mitigate, and deter cyber threats targeted at SLTT computer networks.

The reliance on computers within U.S. society will continue to increase while new and increasingly sophisticated types of internet-connected devices will continue to be relied upon for life-sustaining and activities that support most aspects of modern society. The lack of a collaborative strategy and framework at the SLTT level to address the problem, places SLTT entities and critical infrastructure networks at an increased risk of compromise. This compromise will be realized through the vulnerability of critical U.S. government computer networks. This thesis reviews the strategies being implemented at the federal level to protect critical computer networks. However, can the strategies and

[1] The White House, *Presidential Policy Directive/PPD-21* (Washington, DC: The White House, 2013).

[2] Ibid.

policies implemented at the federal level assist state and local cybersecurity efforts? Can the strategies and polices at the state and local level be leveraged to provide the same level of protection?

In the 2012 Delouse-NASCIO Cybersecurity Study,[3] state Chief Information Officers (CIOs) reported that 92% of state officials feel cybersecurity is very important for the state; only 24% say they are very confident in protecting state's assets against external threats.[4] This lack of confidence can be directly related to the vulnerability of the computer networks to cyber attacks. The study provided the CIOs' interpretation of the value of stolen personal identifiable information (PII). A study by the Ponemon Institute placed a number on the cost of a record during a data breach: "The average cost per lost or breached record is $194 per the Ponemon Institute's 2011 Cost Data Breach Study."[5]

A more extensive and historical examination into government data breach compromises was identified in a January 2014 research study by FireEye, Center for Digital Government, which noted security breaches in the United States accounted for over 608 million records associated with 3,763 data breaches since January 2005. In 2012 alone, 47% of the recorded attacks were identified as malicious attacks (hacking or insider threats). More than 94 million government agency records have been compromised between 2009 and 2012.[6]

The 2014 Deloutte-NASCIO Cybersecurity Study stated that only 24% of the state's' Chief Information Security Officers (CISO) is very confident that their state's information assets are protected against external cyber threats; 55% are confident, while

---

[3] National Association of State Chief Information Officers (NASCIO), *2012 Deloitte-NASCIO Cybersecurity Study, State Governments at Risk: A Call for Collaboration and Compliance* (Lexington, KY: National Association of State Chief Information Officers NASCIO, 2012), Executive Summary, http://www.nascio.org/Surveys/ArtMID/557/ArticleID/106/2012-Deloitte-NASCIO-Cybersecurity-Study-State-governments-at-Risk-A-Call-for-Collaboration-and-Compliance.

[4] Ibid., 3.

[5] Ponemon Institute, *2011 Cost of Data Breach Study: Global* (Traverse City, MI: Ponemon Institute, 2012).

[6] "Advanced Cyber Threats in State and Local Government," 2, accessed February 1, 2015, http://images.erepublic.com/documents/CDG14+SURVEY+FireEye_V2.pdf.

16.3% are not very confident.[7] This survey provides a look into the confidence of state leadership's ability to protect their state's computer network. The confidence level is very low considering the many collaboration and information-sharing initiatives already in-place with federal government departments and agencies. As a result, a balanced comprehensive cybersecurity policy is needed to ensure cooperation and information sharing between federal agencies and the private sector. This cooperation would surely lead to a shared and more effective situational awareness that in turn would enable integrated operational actions to secure this nation's cyber infrastructure.

This study examines the implementation of policies, strategies, operational principles and frameworks to address the cybersecurity protection needs of SLTT entities. The research also examines authorities and a review of state and local fusion centers as a mechanism that could be utilized to prevent, protect, mitigate, and recover from cyber attacks at the state and local level.

B. RESEARCH QUESTION

Should regional state and local fusion centers assist to prevent, mitigate, and deter cyber threats targeted at SLTT[8] entities? This thesis investigates the organizational and individual damage cyber threats can impose upon state and local government (government, finance, education, and critical infrastructure) computer networks. In addition, it examines the benefit of deploying dedicated cyber support teams (jointly manned by state and local, Department of Homeland Security (DHS), and Department of Justice (DOJ) personnel) directly into local and regional fusion centers to absorb a cybersecurity mission and implement strategies and policies designed to prevent, mitigate, and deter cyber threats targeted at SLTT government computer networks.

---

[7] "9326942 NASCIO Cybersecurity Survey," accessed March 6, 2015, http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy_2014.pdf.

[8] "Cybersecurity Workforce Key to Combating Threats," accessed April 22, 2016, http://www.nga.org/cms/home/news-room/news-releases/2014--news-releases/col2-content/cybersecurity-workforce-key-to-c.html. NOTE: this thesis focuses primarily on the state and local components of SLTT. Tribal and territorial components are a part of the acronym but are not the focus of this thesis. Although, any strategy or initiative discussed at the state and local level can surely be scaled or designed to accommodate the tribal and territorial landscape.

The cyber threat to the nation can be intentional or unintentional, arise from a variety of sources, and affect every level of government. All sectors of the country are at risk from nation-state and non-state actors, for criminal and terrorist purposes.[9] This study focuses on regional state and local fusion centers to absorb a cyber mission to handle terrorist and criminal threats. The fusion centers inherent mission is to "correlate the gathering, analysis, correlation, and sharing of threat related information between the federal government and SLTT organizations."[10] State and local fusion centers are uniquely positioned (physically and operationally) to defend against, mitigate, and prevent the cyber threat facing SLTT computer networks.

This research provides the following:

- An analysis of the cyber threat to SLLT entities
- An assessment of applicable current fusion center policies relating to cybersecurity
- An analysis of state fusion centers' ability to accept a new mission focus of cybersecurity defense, mitigation, and analysis, including the establishment of cybersecurity teams or groups resident within the centers
- A proposed strategy for regional fusion centers and state security operation centers to partner with the federal government's departments and agencies in a consolidated cybersecurity collaboration mission

C. LITERATURE REVIEW

The size and complexity of the cyber threat is consistently growing. The challenges America faces in securing cyberspace can be found at all levels of government, public, and private computer domains. In tackling this complex subject, this literature review attempts to summarize the books, articles, congressional reports, and journals related to cybersecurity and information assurance strategies. The review

[9] "Intel Heads Now Fear Cyber Attack More Than Terror," March 13, 2013, http://abcnews.go.com/Blotter/intel-heads-now-fear-cyber-attack-terror/story?id=18719593.

[10] "State and Major Urban Area Fusion Centers," accessed February 11, 2014, http://www.dhs.gov/state-and-major-urban-area-fusion-centers.

examines four areas: the cyber threat facing SLTT entities, fusion centers, leadership thoughts and strategies, and cybersecurity federal policies, governance and laws.

1. Cyber Threats—Government Reporting

This section reviews policies and laws that allow for information sharing between government agencies and amongst industry partners. The Government Accounting Office (GAO) has written extensive articles on cybersecurity covering a wide range of topics. The following articles pertain to the cyber threat: "Threats Impacting the Nation," "Continued Attention Needed to Protect Our Nation's Critical Infrastructure," "Cyberspace Policy," "Challenges Securing the Electricity Grid," and "A Better Defined and Implemented National Strategy is Needed to Address Persistent Challenges." The GAO supports Congress as a bi-partisan organization that investigates federal government departments and agencies to ensure accountability in an effort to make the government more effective and efficient.[11] In support of its oversight mission, the GAO's investigation of the cybersecurity landscape has been comprehensive and revealing.

Cyber threats impacting the nation continue to be a revolving and growing threat of an intentional and unintentional nature. The reports discuss cybersecurity threat sources, types of cyber exploits, the vulnerability of critical infrastructure to cyber attacks, and the number and types of cyber incidents reported to federal agencies. This information is mostly focused on critical infrastructure and government agencies that report incidents to the federal government.

The 18 critical infrastructure sectors rely heavily on computer networks to communicate secure information. The threats against critical infrastructure assets were detailed and provide insight into the daunting task of securing the networks and the information it contains. The federal government has taken a number of steps to secure the networks, such as a Presidential appointment of a Special Assistant to the President for Cybersecurity, DHS issuance of an updated version of the National Infrastructure Protection Plan, and the establishment of the National Cybersecurity and Communications Integration Center (NCCIC) by the DHS in 2009 as a communication

[11] "About GAO," accessed March 6, 2015, http://www.gao.gov/about/index.html.

center to coordinate national response to cyber incidents. However, the GAO Report (*Continued Attention Needed to Protect Our Nation's Critical Infrastructure*) list a number of significant challenges that remain and need to be addressed, although, SLTT entities are not addressed, even though they may be responsible for the security of critical infrastructure networks within their state(s).[12] The GAO discussed how a national strategy was needed to address persistent challenges in support of federal government departments and agencies. A review of cyber incidents reported to government agencies from 2006 to 2012 showed a consistent climb (782%) in cyber incidents. Three key challenges were "designing and implementing risk-based cybersecurity programs at federal agencies, establishing and identifying standards for critical infrastructures, and detecting, responding to, and mitigating cyber incidents."[13] A look at how cybersecurity strategy has evolved was also discussed and details were provided on additional desirable characteristics.

2. Cyber Policy

One of the primary thrusts of the May 2010 White House Cyberspace Policy Review is to "implement coherent unified policy guidance where necessary in order to clarify authorities, roles and responsibilities … across the Federal government."[14] The bill was a policy targeted at the evolving tactics of the adversary. However, the bill, which went through several changes, continues to be in draft in Congress. The lack of movement on this critical legislation comes with a price.

---

[12] U.S. Government Accountability Office, *Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure Statement of Gregory C. Wilshusen, Director, Information Security Issues* (GAO-11-865T) (Washington, DC: U.S. Government Accountability Office, 2011), http://www.gao.gov/assets/130/126702.pdf.

[13] U.S. Government Accountability Office, *Cybersecurity: A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges Statement of Gregory C. Wilshusen, Director Information Security Issues* (GAO-13-462T) (Washington, DC: U.S. Government Accountability Office, 2013), http://www.gao.gov/products/GAO-13-462T.

[14] The White House, *Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communication Infrastructure* (Washington, DC: The White House, 2009), 10, https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

In May 2009, during his speech on Cybersecurity, President Obama detailed a McAfee estimate that the global cost of cybercrime at approximate $1 trillion.[15] During the deliberations on the Cybersecurity Act of 2012, Senators Lieberman and Collins referenced a Symantec estimate that the theft of intellectual property to American companies cost $250 billion a year.[16] The speed at which the cyberspace domain evolves and the number of adversaries (big and small) attempting to take advantage of America's lack of policy, security, and resiliency makes cybersecurity one of America's greatest security challenges. Securing the web against cyber attacks is a national priority as cyber criminals attempt to steal U.S. critical information and trade secrets.

Although Congress has failed to act, President Obama continues to push for increasing policies and directives, as the Administration has produced an executive order (EO) "Improving Critical Infrastructure Cybersecurity" and PPD-21 "Critical Infrastructure Security and Resilience" to help secure America's cyber infrastructure. PPD-21 states, "The Federal Government shall work with critical infrastructure owners and operators and SLTT entities to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure"[17] The policy combines the efforts of all three organizations to protect critical infrastructure assets and how a unity of effort is needed to advance and strengthen critical infrastructure security and resilience.

In February 2015, President Obama signed the Promoting Private Sector Cybersecurity Information Sharing EO. Presently, "most private sector information sharing is conducted through Information Sharing and Analysis Centers (ISACs) … these groups primarily operate on a sector model, where companies within a certain sector (i.e., financial services, energy, aviation, etc.) share information about threats within that

[15] The White House, "President Obama on Cybersecurity" (transcript, The White House, May 29, 2009).

[16] "Psychology Behind Intellectual Property Theft by Corporate Insiders," accessed 14 October 2012, https://www.symantec.com/about/newsroom/press-releases/2011/symantec_1207_01.

[17] "Presidential Policy Directive—Critical Infrastructure Security and Resilience," accessed March 6, 2015, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

sector."[18] The ISAC model has been adopted by the energy, communications, information technology (IT), states, and financial sectors to name a few. The model is not a totally inclusive mechanism for information sharing because many companies do not fit within an established sector. As a result, some companies have attempted to develop their own information sharing and analysis organizations (ISAOs). Like ISACs, the purpose of ISAOs is to gather, analyze, and disseminate threat information, but unlike ISACs, they are not' sector-affiliated. The EO directs DHS to encourage the development of ISAOs.[19]

The Administrations initiatives are strategies and guidelines that identify critical infrastructure sectors and advance the idea of a national unity of effort. The authorities and directives attempt to "refine and clarify roles and relationships across the Federal Government."[20]

3. Leadership Thoughts and Strategies

Speaking in September 2012, Secretary of Homeland Security Janet Napolitano said, "threats to the U.S. cyber infrastructure were one of the most serious and rapidly evolving threats the nation faces."[21] Four months later, in January 2013, the Secretary said, "We shouldn't wait until there is a 9/11 in the cyber world. There are things we can and should be doing right now that, if not prevent, would mitigate the extent of damage."[22]

One of the first to speak of this cyber 9/11 was Secretary of Defense Leon Panetta. In October 2012, Secretary Panetta, speaking at the annual awards dinner for the non-profit organization, Business Executives for National Security, stated, "A cyber-

---

[18] "Information Sharing and Analysis Organizations (ISAOs)," accessed April 9, 2016, https://www.dhs.gov/isao.

[19] "Executive Order—Promoting Private Sector Cybersecurity Information Sharing," accessed March 21, 2015, https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

[20] "Presidential Policy Directive—Critical Infrastructure Security and Resilience."

[21] Janet Napolitano, "Cyber Attacks One of the Most Serious Threats," Infosecurity, September 11, 2012, www.Infosecurity-Magazine.com.

[22] Janet Napolitano, "U.S. Homeland Chief: Cyber 9/11 Could Happen "Imminently,"" Reuters, January 24, 2013, www.Reuters.com/article.

attack perpetrated by nation states or violent extremist groups could be as destructive as the terrorist attack of 9/11."[23]

Philip Reitinger, former Deputy Under Secretary for DHS National Protection and Programs Directorate (NPPD), thinks the United States should implement a "cyber ecosystem" … where "cyber devices have innate capabilities that enable them to work together to anticipate and prevent cyber attacks in near real-time."[24] Reitinger advocates an ecosystem where "cyber devices communicate in near real-time with each other about attacks, and take coordinated security hardening response actions consistent with a defined policy framework, allowing many security risks to be managed proactively and dynamically."[25]

General Keith Alexander, director of the National Security Agency and the commander of U.S. Cyber Command said, "The U.S. must work with its partners in industry and its allies to solve the problem."[26] Gen. Alexander is endorsing a whole government approach, combined with industry and international partners, to solve the nation's cyber problems. Gen. Alexander also proposes a "defensible architecture,"[27] a virtual cloud-based network defense and offense, a process that takes the cyber fight to the adversaries.

Franklin Kramer, a senior political appointee in two administrations, a former Distinguished Research Fellow at the National Defense University, and principal author of *Cyberpower and National Security*, echoed Gen. Alexander's thoughts stating, "the U.S. must create an effective national and international strategic framework for the

---

[23] Gopal Ratman, "Cyberattacks Could Become as Destructive as 9/11: Panetta," Bloomberg, October 11, 2012, http://www.bloomberg.com/news/articles/2012-10-12/cyberattacks-could-become-as-destructive-as-9-11-panetta.

[24] Philip Reitinger, *Enabling Distributed Security in Cyberspace, Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action, Department of Homeland Security* (Washington, DC: Department of Homeland Security, 2011), 5, https://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf.

[25] Ibid., 6.

[26] Cheryl Pellerin, "Cybersecurity Involves Federal, Industry Partners, Allies, American Forces Press Service," 1, accessed December 15, 2012 http://archive.defense.gov/news/newsarticle.aspx?id=118479.

[27] Ibid., 3.

development and use of cyber as part of an overall national security strategy."[28] Kramer also believes the United States should adopt a cyber warfare or "computer network attack" (CNA) strategy.[29] He believes CNA strategies should attempt to reduce classifications and enhance integration to provide comprehensive offensive strategies to deter U.S. adversaries.

One key difference between the approach identified by Alexander and Kramer but not mentioned directly by Reitinger is the idea of offensive attacks against an adversary. Both Alexander and Kramer are from the Department of Defense (DOD) community. The concept of offensive operations, designed to deter an enemy, is not only considered but plays a big role in the defense of the cyber domain. Reitinger's cyber ecosystem adheres to a cooperative approach amongst systems to communicate when attacks happen. This strategy is designed to mitigate and possibly deter the adverse effects of a cyber-attack.

4. Fusion Centers

The National Security Strategy of May 2010 states, "To prevent acts of terrorism on American soil, we must enlist all of our intelligence, law enforcement, and homeland security capabilities. We will continue to integrate and leverage state and major area fusion centers that have the capability to share classified information"[30] DHS initiated a program in 2010 to pass secret-level classified information with industry officials through the use of fusion centers. The Cybersecurity Partner Local Access Plan (CPLAP) was designed to allow industry officials the ability to go to their local fusion center and review classified information, and at the same time, build a relationship between critical infrastructure and key resource partners with fusion center officials.[31] The fusion center public-private partnership continued to build in July 2011 in the Northeastern part of the

---

[28] Franklin D. Kramer, *Policy Recommendations for a Strategic Framework* (Washington, DC: Cyberpower and National Security, National Defense University Press, 2010), 7.

[29] Ibid., 14.

[30] The White House, *National Security Strategy* (Washington, DC: The White House, 2010), http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

[31] "DHS, Industry to Try Fusion Centers for Classified Data Swap," accessed February 11, 2014, http://fcw.com/Articles/2010/03/16/Web-cyber-threat-fusion-center.aspx?p=1.

United States as the fusion centers in Delaware, Virginia, Maryland, New Jersey, and Pennsylvania met with their public private partners to collaborate on information-sharing practices and threat information regarding critical infrastructure.[32] In 2012, on the West Coast, the Northern California Regional Center (NCRIC) held a cybersecurity roundtable with partners from the financial and IT sectors.[33] This partnership, led by DHS, continues to grow throughout the country. The importance of this partnership is further examined in a section within this thesis.

Although an emphasis was placed on using the fusion centers to protect the homeland, provide an atmosphere of collaboration, and increase information sharing between the federal government and SLTT entities; fusions centers were given a failing grade on the October 3, 2012 by the U.S. Senate Permanent Subcommittee on Investigation. The report found "that DHS' work with those state and local fusion centers has not produced useful intelligence to support federal counterterrorism efforts."[34] The report is completely contrary to the National Preparedness Report (NPR), which key findings stated, "A network of state and regional fusion centers and Joint Terrorism Task Force (JTTF) has significantly improved analytical and information sharing capabilities among law enforcement, homeland security, and Intelligence Community entities at all levels of government."[35] The NPR used a survey to obtain its analysis. The Subcommittee on Investigations reviewed reports, visited fusion centers, and analyzed budget decisions, in comparison to DHS requirements. Although the report is very critical of the fusion centers, the recommendation section holds optimism that the problems can be corrected.

---

[32] "Fusion Centers and Public-Private Collaboration," accessed February 17, 2014, http://ise.gov/blog/major-thomas-souchek/fusion-centers-and-public-private-collaboration.

[33] "Fusion Centers and Private Sector Come Together on Cybersecurity," accessed January 15, 2014, https://www.ise.gov/blog/mike-sena/fusion-centers-and-private-sector-come-together-cybersecurity.

[34] United States Senate, *Permanent Subcommittee on Investigations, Federal Support for and Involvement in State and Local Fusion Centers* (Washington, DC: United States Senate, 2012), Executive Summary, www.CDN.GOVEXEC.com.

[35] Department of Homeland Security, *National Preparedness Report* (Washington, DC: Department of Homeland Security, 2012), 12, http://www.fema.gov/media-library-data/20130726-1833-25045-2705/national_preparedness_report_20120330_v2_1.pdf.

The first recommendation by the Subcommittee on Investigations was for DHS to "conform its efforts to match its counterterrorism statutory purpose, or redefine DHS' fusion center mission."[36] Four months earlier, a change in fusion centers' security challenges were echoed at the Naval Postgraduate School in Monterey, California. The Center for Homeland Defense and Security Fusion Center Leaders Program (FCLP) conducted June 5–8, 2012, highlighted the "Shifting Security Challenges."[37] Twenty-five fusion center leaders gathered to share ideas on information-sharing strategies that could be utilized across the state and local fusion center network.[38]

5. State, Local, Tribal, and Territorial

As the nation goes about trying to protect its information, a key concern within the cyber community is deciding the best way to protect the SLTT organizations. Has the federal government adequately supported the SLTT entities? Or, does the federal government have the task to coordinate and protect state and local entities?

The March 2012 National Preparedness Report stated, "Cybersecurity was the single core capability where states had made the least amount of overall progress. In addition, DHS's 2011 Nationwide Cybersecurity Review highlighted gaps in cyber-related preparedness among 162 state and local entities."[39] The ability to secure SLTT networks normally takes a back seat to the highly publicized attacks that affect critical infrastructure, or the energy or the defense industrial base. A 2012 Deloutte-NASCIO Cybersecurity Study,[40] state CIO's reported that 92% of state officials think cybersecurity is a priority and only 24% think their state is positioned to protect the state resources from a cyber-attack.[41]

---

[36] United States Senate, *Permanent Subcommittee on Investigations, Federal Support for and Involvement in State and Local Fusion Centers*, 106.

[37] "Fusion Centers Are Meeting Shifting Security Challenges," June 29, 2012, https://www.chds.us/c/item/771.

[38] Ibid.

[39] FEMA, *2012 National Preparedness Report (NPR)* (Washington, DC: FEMA, 2012).

[40] National Association of State Chief Information Officers (NASCIO), *2012 Deloitte-NASCIO Cybersecurity Study, State Governments at Risk: A Call for Collaboration and Compliance*, Executive Summary.

[41] Ibid., 3.

What is lacking in the current research is a consolidated strategy and framework on how to best incorporate the cyber threat faced by SLTT entities into the federal and private sector strategy to protect the cyber domain. Further analysis is also needed to determine if state and local fusion centers have a role in the fight against cyber threat actors in the protection and information security of the SLTT cyber infrastructure.

D. RESEARCH DESIGN

This thesis examines a whole-of-government approach to analyze a strategy and policy that will protect SLTT entities better from cyber threats.

The research question addresses the viability of state and local fusion centers' ability to absorb an adjunct mission and implement strategies and policies designed to prevent, mitigate, and deter cyber threats targeted at SLTT entities. This thesis uses a qualitative research method to interpret new insights into the cyber threat phenomenon facing the nation. The study identifies key cybersecurity shortfalls in SLTT cyber defense strategies, and suggests new concepts and strategies to protect state and local computer networks. The research can be used to judge the effectiveness of federal, executive, and homeland security policies, strategies, and directives to identify gaps and determine effective policies, strategies, and frameworks to address the cyber threats targeted at SLTT entities.

Secondary data collection centers on the literature review. The collection of literature includes government policies, GAO reports, Congressional Research Service (CRS) reports, studies, information-sharing initiatives, policies, executive actions, and other data sources as appropriate. Visits to fusion centers in Baltimore, Maryland and San Francisco, California will be used to get a first-hand look at the fusion centers' missions, capabilities, processes, and procedures. These locations were selected because of the proximity of the fusion centers to the author's residence and the Naval Postgraduate School in Monterey, CA. The analysis of the procedural data, observed during the visits to the fusion centers, allows for an assessment of the center's' capabilities in comparison to their documented strengths and weaknesses, as detailed in the literature review. The visits to these locations also provide insights into the ability of the fusion centers to take

on an adjunct mission of cyber security. Combined with the analysis of the resource material, this research allows for an assessment of the types of cyber threats targeted at state and local government departments.

A review of the literature, an analysis of the cyber threat to SLTT entities, an examination of the current cybersecurity policies, and an analysis of the state and local fusion center mission allow for the development of a strategy, policy, and framework to address the thesis hypothesis.

The goal of this thesis is to analyze the cyber threat to the nation and to SLTT computer networks, introduce fusion centers as a viable cybersecurity option, and examine their ability to accept a new mission focused of cybersecurity defense, mitigation, and recovery. Lastly, this thesis proposes a strategy that would incorporate cybersecurity teams into fusion centers in an effort to protect SLTT entities better from cyber threats. The cybersecurity teams' concept is adopted from the combat support group (CSG) concept used by agencies within the intelligence community to provide specialized teams to help strengthen specific mission and operational requirements needed to accomplish the operational and strategic goals.

E. CHAPTER OVERVIEW

The chapter examined the cyber threat to the nation, to SLTT entities, the possible role of fusion centers in countering the threat, and a strategy or framework to address the cybersecurity protection of SLTT computer networks.

Chapter II examines the cyber threat. What is the seriousness of the threat? Is a collaborative approach to identify, protect, deter, and minimize the threat working to secure the nation's computer networks? The chapter reviews specific polices and strategy used to strengthen cybersecurity information sharing and collaboration. An analysis of what has worked and has not worked is provided. The purpose is to frame the problem and start the process of outlining opportunities for improvement. The chapter closes by examining the effect the threat is having on SLTT computer networks.

Chapter III focuses on the challenges faced by SLTT entities and state CIOs. A clear identification of the cyber threat to SLTT networks and the challenges also include a review of the currently on-going collaboration efforts and the options and strategies utilize to provide support to SLTT governments. The chapter introduces the fusion centers as a viable option to absorb an additional cybersecurity mission capability.

Chapter IV will focus on the national response to the cyber threat and examine the cybersecurity strategies, policies, EOs and laws that are primarily designed to support information sharing at the federal level and between public and private industry partners. A review of the operational framework will be analyzed to identify if the standard can be used across the cyber landscape.

Chapter V examines the cyber threat and the seriousness of the threat to state and local governments. It discusses the various programs, partnerships, and accompanying policies that allow federal government assets, information, and capabilities to be leveraged by SLTT governments.

Chapter VI examines the fusion centers from a cyber perspective. The chapter analyzes the roles and responsibilities of the organizations with the authority or responsibility to assist SLTT entities against the cyber threats.

Finally, Chapter VII provides conclusions from the research, answers the research question, and offers a comprehensive approach to cybersecurity in the fight against cyber threats targeted at SLTT entities.

THIS PAGE INTENTIONALLY LEFT BLANK

II. THE CYBER THREAT TO THE NATION

This chapter examines the cyber threat to the nation and its impact on America's critical infrastructure, government, and state and local computer networks. The cyber threat to America's critical infrastructure, government networks, electrical grids, finance, education, military, and its citizens is not new. The threat happens daily and it appears it will continue on into the future. The cyber threat happens under the cloak of secrecy. The adversaries are able to hide their identity while stealing intellectual property, financial information, and personal identifiable information. The adversaries test their trade by attempting to overwhelm by denying access to the network by shutting down computer servers that house financial data, that operate dams and electrical grids, or that safeguard military networks. Networks that house critical information that allows the country to continue to advance its economic and national security are being targeted on a daily, hourly basis. The cyber adversary is illusive and understands the threat environment. Since the size of the internet is so vast, likewise is the opportunity space for the hacker, the criminal, and the nation-state actor. The hacktivist is someone or a group who hacks into the computer as a form of protest. The hacktivist is motivated mostly by political gain and not for profit. The cyber criminal (a person or group) uses the computer to steal a person's identity, hack into financial accounts, sends bogus emails to gain access and control of a victim's computer and infect their computer with a malicious virus. The nation-state actors are funded and resourced very well. They can employ hackers, military and civilian computer personnel to gain access to computers that hold PII, financial data, intellectual property, and other critical information. The hacker, cyber criminal, and nation-state actor often times take advantage of software vulnerabilities that can negatively affect computer networks.

A. NETWORK VULNERABILITIES

In 2012, the *Shamoon virus*, also known as W32.Disttrack, was a threat that targeted the energy sector. The destructive malware corrupted files on a compromised computer and then overwrites the master boot record (MBR) and renders the computer

useless.[42] The virus was responsible for an attack on 30,000 Saudi Aramco (oil and gas enterprise in Saudi Arabia) computers. The virus was not used for personal financial gain, or to steal PII data but was designed and targeted at the oil company to damage the organization.[43] Then Secretary of State, Leon Panetta stated, "The 'Shamoon' virus … was probably the most destructive attack the business sector has seen to date." He went on to say, "While this kind of tactic isn't new, the scale and speed with which it happened was unprecedented."[44]

The *Heartbleed vulnerability* burst onto the computer scene in April 2014. The bug is a serious vulnerability to the internet, as it exposes weaknesses in the OpenSSL (secure socket layer) cryptographic software library. Since the internet is used by so many users, security must be in place to ensure that email, instant messaging (IM) and virtual private networks (VPNs) can communicate securely, and SSL is one form of software that allows for secure communications. OpenSSL allows for an encryption to be applied to the internet to allow for increased security; in essence, it protects the electronic traffic on websites and electronic devices. This encryption provides security over internet applications, such as email, IM, and web-based browsing to name a few.[45] Netcraft, an internet service company based in England, estimated that 17.5% of SSL sites, accounting for around half a million certificates, were vulnerable to the Heartbleed bug.[46] The Heartbleed vulnerability allows the attacker to act as a spy; they can steal data, hide their identity, or impersonate another person's identity. This vulnerability can provide access to the memory and controller data of the servers and clients. About the time the Heartbleed vulnerability had been contained, the Bash vulnerability seemed to appear.

---

[42] "The Shamoon Attacks," accessed February 18, 2016, http://www.symantec.com/connect/blogs/shamoon-attacks.

[43] "Why the Shamoon Virus Looms as Destructive Threat," accessed February 18, 2016, http://www.usatoday.com/story/cybertruth/2013/05/16/shamoon-cyber-warfare-hackers-anti-american/2166147/.

[44] Dino Grandoni, "The Most Destructive Virus to Ever Hit a Business?," *The Huffington Post*, accessed February 18, 2016, http://www.huffingtonpost.com/2012/10/11/shamoon-virus-leon-panetta_n_1960113.html.

[45] "Heartbleed Bug," accessed February 10, 2015, http://heartbleed.com/.

[46] "Half a Million Widely Trusted websites Vulnerable to Heartbleed Bug," accessed February 10, 2015, http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html.

In September 2014, the *Bash Bug vulnerability* was a bug that affected UNIX and LINUX operating systems. The operating system (a critical part of the computer) is the software that allows the user to talk to the computer without knowing the computer language. The bug, also known as ShellShock, targets the shell of the software to allow an attacker to gain access. The vulnerability, when exploited, would allow attackers to steal information and control the computer or gain access to the entire computer network.[47] The magazine *Information Week* estimated the Heartbleed bug affected 500 million computers. The magazine quoted the *BBC* (British Broadcasting Corporation) as stating the same number could also be affected by the Bash vulnerability.[48] The ShellShock vulnerability dates back to 1994. Another bug that has infected computer systems in the past is the Conflicker virus, which has re-emerged as a new vulnerability on the cyber landscape.

The *Conficker worm* was first noticed in 2008,[49] and takes advantage of security flaws in Microsoft Office. The computer worm is a standalone malware program that replicates itself to affect other computers.[50] The worm travels on the internet searching for flaws in operating systems to infect and control other computers. Many experts say 'it is the worst computer infection since the Slammer worm in 2003, and as many as nine million computers could have been infected.[51] Worms are different from viruses, as they can operate independently and do not require any human involvement. Worms also allow infected computers to act together to form botnets (an army of computers). This functionality provides the cyber criminals the ability to scale their operations and to hide their identity even more. Both worms and viruses take advantage of software

---

47 "ShellShock: All You Need to Know about the Bash Bug Vulnerability," accessed February 10, 2015, http://www.symantec.com/connect/blogs/shellshock-all-you-need-know-about-bash-bug-vulnerability.

48 "Protecting Yourself from the Conficker Worm," accessed February 12, 2015, http://home.mcafee.com/root/landingpage.aspx?affid=0&lpname=18310&cid=54857&culture=en-US&legacylangcd=en-us.

49 Ibid.

50 "What Is a Computer Worm," accessed February 12, 2015, http://www.pctools.com/security-news/what-is-a-computer-worm/.

51 "Worm Infects Millions of Computers Worldwide," accessed March 14, 2014, http://www.nytimes.com/2009/01/23/technology/internet/23worm.html?_r=0.

vulnerabilities known by the cyber criminal. However, many vulnerabilities have not yet been discovered. These vulnerabilities are known as zero-day exploits.

A *zero-day exploit* refers to a "hole in the software that is unknown to the vendor."[52] The zero-day exploit is a race against time between the cyber criminal who attempts to exploit the software and the vendor who attempts to discover the vulnerability and close the software hole. A perfect example of the zero-day exploit was witnessed in January 2015, when Adobe Systems disseminated a critical patch for their popular Adobe Flash software. The vulnerability had been discovered by cyber criminals who were taking advantage of the hole in the software to launch malicious malware attacks, using drive-by downloads and malicious ads.[53] Unknown computer users who visit legitimate websites and unknowingly click on malicious advertising were infected with the virus. Adobe needed to work fast to minimize the effects of the compromised software. However, the criminals were working even faster, as Adobe eventually had to patch three vulnerabilities in three weeks with regards to this exploit.[54]

The primary reason for focusing on vulnerabilities in networks is not only to identify the vulnerability but also to pose the question, how prepared are SLTT entities prepared to defend against the vulnerabilities? A 2014 FireEye report stated, "Strapped for resources, state and local governments are a prime target for the pervasive and sophisticated threats launched by stealthy cyber criminals."[55] Limited resources (financial, personnel, capabilities, etc.) to defend against cyber threats provide a greater opportunity for a successful attack. What strategy is needed to prevent, mitigate, and deter cyber threats targeted at SLTT government computer networks?

---

[52] "Adobe Pushes Critical Flash Player Update to Fix Latest Zero-Day," January 26, 2015, http://www.pcworld.com/article/2875252/adobe-pushes-critical-flash-player-update-to-fix-latest-zeroday.html.

[53] "Adobe Confirms Patch for Newest Zero-Day Vulnerability," February 2, 2015, http://www.csoonline.com/article/2878778/application-security/adobe-confirms-patch-for-newest-zero-day-vulnerability.html.

[54] "Anonymous Hackers, Your Unmasked Face Picture Might Be in This List!," accessed February 12, 2015, http://cyberwarzone.com/anonymous-hackers-unmasked-face-picture-might-list/.

[55] Center for Digital Government, *Advanced Cyber Threats in State and Local Government* (Folsom, CA: Center for Digital Government, 2014), http://nascio.org/events/sponsors/vrc/Advanced%20Cyber%20Threats%20in%20State%20and%20Local%20Government.pdf.

B. THREAT ACTORS

> There are only two types of companies: those that have been hacked and those that will be.
>
> ~ FBI Director Robert Mueller

Director Mueller's comments at the RSA Conference in San Francisco, California echoes the severity of the IT threat to the nation. Director Mueller went on to say, "Terrorism does remain the FBI's (Federal Bureau of Investigations) top priority, but in the not too-distant-future we anticipate that the cyber threat will pose the greatest threat to our country."[56] Today, terrorists utilize technology to enable an operation to be carried out (propaganda, training, financial support, cyber attacks, etc.).[57] From a cyber perspective, technology allows the cyber attackers to mask their identity, expand their reach, multiply their impact on computer networks and systems, and increase the destructive effect on individual privacy, business proprietary information, critical infrastructure, and government departments and agencies. This section examines the threat from nation-state actors, terrorist, criminals, and hacktivists.

1. Nation-State

> Cyber theft is real theft, and we will hold state-sponsored cyber thieves accountable as we would any other transnational criminal organization that steals our goods and breaks our laws.[58]
>
> ~ Assistant Attorney General for National Security John Carlin

On May 19, 2014, the U.S. government charged five Chinese military hackers for hacking, stealing economic secrets, and other offenses directed at U.S. nuclear power and

---

[56] Ibid.

[57] "Terrorism: Role of Technology in Contemporary Terrorism," accessed February 19, 2016, http://criminaljusticeonlineblog.com/12/terrorism-role-of-technology-in-contemporary-terrorism/.

[58] "Five Chinese Military Hackers Charged with Cyber Espionage against U.S.," accessed February 12, 2015, http://www.fbi.gov/news/news_blog/five-chinese-military-hackers-charged-with-cyber-espionage-against-u.s.

critical infrastructure industries.[59] The charges date back to 2006 and specifically name a military unit with the Chinese People's Liberation Army.

In April 2014, a British newspaper reported an FBI investigation into a "sophisticated high-level" cyber-attack attributed to the Russians targeting U.S. financial institutions. Wall Street business J.P. Morgan Chase was one of two financial institutions named in the attacks.[60]

In November 2014, DHS identified a "BlackEnergy" malware that had been used against several industrial control system critical infrastructure companies in the United States. DHS stated the activity could be traced back to 2011 and had been attributed to a Russian cyber espionage group named "Sandworm." The Trojan horse style of malware had not been activated but was found on several organizations networks.[61]

In November 2014, a cyber espionage group named the Guardians of Peace (#GOP) targeted Sony Picture Entertainment and hacked into their email accounts and stole PII data from the organization. The #GOP leaked PII data to the public to embarrass Sony Executives in response to a film "The Interview," which depicts two Americas attempting to assassinate the North Korean leader Kim Jong Um. The cyber-attack designed to embarrass and threaten Sony initially worked, as Sony cancelled the release of the movie in theaters nationwide.[62]

Dating back to the beginning of 2012, the Iranian government had been confirmed as targeting the U.S. financial institutions with persistent distributed denial of service attacks (DDoS). The Qassam Cyber Fighters, an organization attributed to the Government of Iran, states, "it is retaliating for the anti-Islamic video made in America

---

[59] Ibid.

[60] "Charges Unsealed against Five Alleged Members of Al Qaeda Plot to Attack the United States and the United Kingdom," accessed November 1, 2013, http://www.fbi.gov/newyork/press-releases/2010/nyfo070710a.htm.

[61] Jack Cloherty and Pierre Thomas, "'Trojan Horse' Bug Lurking in Vital U.S. Computers," *ABC News*, November 7, 2014, http://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers-2011/story?id=26737476.

[62] "Timeline: North Korea and the Sony Pictures Hack," accessed February 12, 2015, http://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/.

that has caused protests in Muslim countries."[63] In a DDoS attack, the attacker bombards an online service with traffics that render it unavailable to other sources.[64] In addition, in the banking business, online banking has become a normal, convenient, and secure way to bank across America. The group Cyber fighters of Izz ad-din Al quassam took responsibility for the attack via a Pastebin posting.[65] However, "the scale, the scope and the effectiveness of the attacks were too sophisticated for the Cyber fighters." U.S. intelligence officials were quoted as saying the group is a cover for Iran.[66] The U.S. financial institutions, BB&T, Capital One, Citi, and Chase are some of the banks that have been affected by DDoS attacks.

In September 2014, Robert Anderson, the executive assistant director for the FBI's Criminal, Cyber, Response, and Services branch said during his testimony to Congress, "that virtually all agencies of the U.S. government have in some way been hacked." Susan Spaulding, undersecretary of DHS's National Protections and Program Directorate states, that in only nine months of 2014, "the National Cybersecurity and Communications Integration Center (NCCIC) had responded to more than 600,000 cyber incidents, issued more than 10,000 actionable alerts, and deployed 78 on-site teams to provide assistance to affected organizations."[67] The words from the FBI are very troubling. If the federal government computer networks are being consistently breached, then, how secure are SLTT government computer networks?

---

[63] Siobhan Gorman, "Iran Renews Internet Attacks on U.S. Banks," *Wall Street Journal*, October 18, 2012, sec. Tech, http://www.wsj.com/articles/SB10000872396390444592704578063063201649282.

[64] "Digital Attack Map," accessed February 12, 2015, http://www.digitalattackmap.com/understanding-ddos/.

[65] Todd Reagor, "DDOS Attacks on Chase Point to Iran Hacker Group," *Rivalhost Blog*, September 21, 2012, https://www.rivalhost.com/blog/ddos-attacks-on-chase-point-to-iran-hacker-group/.

[66] Nicole Perlroth and Quentin Hardy, "Online Banking Attacks Were Work of Iran, U.S. Officials Say," *The New York Times*, January 8, 2013, http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html.

[67] "Is There Any Part of Government That Hasn't Been Hacked Yet?," accessed February 19, 2016, http://www.nextgov.com/cybersecurity/2014/09/there-any-part-government -hasnt-been-hacked-yet/93704/.

2. Terrorist

Cyber terrorism is defined as "computer-based attacks aimed at disabling vital computer systems so as to intimidate, coerce, or harm a government or section of the population."[68] A cyber terrorist would be the individual or group performing the malicious cyber-attack. The December 2014 cyber attack against Sony pictures stole personal information for more than 6,000 Sony employees and posted four unreleased Sony films to the internet. A group called #GOP took credit for the attack. The attack threatened Sony Pictures that additional information would be stolen and released if the company went ahead with the release of their movie, "The Interview."[69] The plot of the movie revolved around an attempt to kill the leader of North Korea; hence, the supposed reasoning behind the #GOP targeting Sony pictures. Although North Korea denied any direct responsibility for the cyber-attack, the country commented on the actions by the #GOP as "a righteous deed of supporters and sympathizers."[70]

One of the first cases of cyber terrorism may be the Stuxnet malware that not only targeted computers but physically destroyed the equipment the computers controlled at the Natanz uranium enrichment plant in central Iran. The cyber-attack was initially launched against employees (a common tactic used to infiltrate a computer network) of industrial control system companies connected to Natanz. This sophisticated attack was nicknamed the world's first digital weapon and caused centrifuges used to enrich uranium to fail.[71]

Cyber terrorism can be performed by nation-states, criminals, or hackers in an effort to compromise governments, military, financial institutions, or critical

---

[68] "Cyberterrorism," accessed February 18, 2016, http://dictionary.reference.com/browse/cyberterrorism?s=t.

[69] "FBI Investigating Cyber-Attack on Sony Pictures," accessed February 18, 2016, http://www.cbsnews.com/videos/fbi-investigating-cyber-attack-on-sony-pictures/.

[70] Ben Child, "North Korea Says Sony Cyber-Attack May Be 'Righteous' Work of Its Supporters," *The Guardian*, December 8, 2014, sec. Film, http://www.theguardian.com/film/2014/dec/08/north-korea-sony-cyber-attack-the-interview.

[71] Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *WIRED*, November 3, 2014, http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

infrastructure assets. The opportunity space is limitless and can only be restricted by the capability and motivations of the cyber terrorist.

3. Criminals

They are known by the name Solo, Sabu, TFlow,Viral, Raven, and Xiao, just to name a few. They have been credited with hacking military computers, infiltrating telephone lines to win radio contests, creating computer worms, and hacking corporations, government, religious organizations, stealing identities, and using direct DDoS attacks against financial institutions and other corporations. Most of these groups or individuals are loosely organized and have little to no allegiance to one another. They treat cyber as a business opportunity only aligning with those temporarily to benefit a certain cause or particular theft. The cyber criminal has various tools and techniques at their disposal. Moreover, their area of operations is vast—the internet—allows for ease of movement, concealment of identities, recruitment, and collaboration.

The cyber criminal is not an everyday computer geek. The cyber criminal looks at the return on investment (ROI) and makes a determined effort to cash in on the opportunity. The ability to hack into a computer from a distant location and steal proprietary information, PII, military plans, aerospace secrets, technology, etc,, and while at the same time, disguising an individual's identity to decrease the chances of being caught, provides a great ROI. Many people, organizations, businesses, and countries are willing to pay a significant amount for the cyber criminal's service. However, the cyber criminals are not the only groups and organizations looking to gain a high ROI and benefit from it. Hacktivist are positioned to take advantage of the same opportunities, and similar to the cyber criminals, they have the skills and capabilities to take advantage of weaknesses and vulnerabilities in computer networks.

4. Hacktivist

Hacktivism is a form of political motivated cyber attack and can be used to promote political means, human rights, government abuse of power, privacy, and freedom of speech to name a few. Hacktivists use several cyber-attack methods: blocking access to websites, defacing of websites, identity theft, virtual sit-ins, and website

hijacking.[72] Hacktivists and terrorists can both be considered criminals. Anonymous and Lulzsec are considered two of the more popular hacktivist groups.[73] Dating back to 2010, Anonymous has been credited with more than 95 cyber attacks. The attacks have been targeted at Sony Playstation, WikiLeaks-Operation Payback (Julian Assange), the Church of Scientology, Iranian elections, Arab Spring activities, U.S. banks (Empire State), Facebook, Wall Street, social media (Op Deepthroat), the Vatican, and the National Security Agency (NSA) document release to name a few.[74] Anonymous appears to have no boundaries; the group moves throughout the world indiscriminately using the computer to promote a political ideology and the cyber-attack as its freedom of expression.

LulzSec (Lulz Security) was a hacking group that gained notoriety with the 2011 Sony network intrusion. The group was also known for its hacking into PBS (Public Broadcasting Service), Infragard and shutting down the CIA (Central Intelligence Agency) website. The small group organized itself by specialty (public relations, software tools, networks, botnets, and DDoS) and was one of the first hacking groups to brand itself and publicize its exploits.[75] LulzSec's success was short-lived as its leader Hector Monsegur, known as Sabu, was arrested by the FBI for cyber crime. It is reported that Sabu then helped the FBI to find and arrest some of his friends in London, New York, and around the world.[76] This activity not only brought the activities of the group to an end, but it also put a dent in the operations of Anonymous.

Groups of hacktivists are still very prevalent throughout the world. The internet is their area of operations, and the access and popularity of social media has enabled them

---

[72] "Verizon Report, the Wind of Hacktivism Pushes Cybercrime," March 22, 2012, http://securityaffairs.co/wordpress/3524/cyber-crime/verizon-report-the-wind-of-hacktivism-pushes-cybercrime.html.

[73] "Hacktivism: Good or Evil?," accessed February 18, 2016, http://www.computerweekly.com/opinion/Hacktivism-Good-or-Evil.

[74] *Wikipedia*, s.v. "Timeline of Events Associated with Anonymous," last modified May 7, 2016, https://en.wikipedia.org/wiki/Timeline_of_events_associated_with_Anonymous.

[75] Damon Poeter, "50 Days of Mayhem: How LulzSec Changed Hacktivism Forever," PCMag.com, accessed March 3, 2016, http://www.pcmag.com/article2/0,2817,2387716,00.asp.

[76] *Wikipedia*, s.v. "LulzSec," February 25, 2016, https://en.wikipedia.org/w/index.php?title=LulzSec&oldid=706907873.

to scale their operations and provide a voice to their platform or political cause. The availability of the internet provides for unlimited possibilities and endless targets of opportunity.

This chapter has focused on the cyber threat. As discussed, U.S. government officials have commented that China, Russia, Iran, and North Korea have all targeted the United States with cyber attacks. The FBI, DHS, and the intelligence community partners all play a role in protecting the countries' computer networks. The combined threat posed by software vulnerabilities, nation-state actors, criminals, and hacktivists provide an increasingly tough challenge to U.S. cyber defenders. The threat is compounded by weaknesses in computer networks that render federal and critical infrastructure systems vulnerable to cyber attacks. These vulnerabilities were highlighted by the threat from Heartbleed, Bash, Conficker, and zero-day vulnerabilities. These challenges will not go away and the actions of the federal, state, and local governments, along with the cooperation with public and private industry, will be required to protect U.S. computer networks. As stated previously, if the federal government computer networks are being consistently breached (as stated by the FBI's executive assistant director for cyber, Robert Anderson) then, how secure are SLTT government computer networks? Figure 1 describes the evolving cyber security threat. The information highway will continue to grow with more and more users. If history is any indicator, the cyber threat will also continue to increase. The need for a comprehensive approach to cybersecurity at all levels of government is needed to deter the threat.

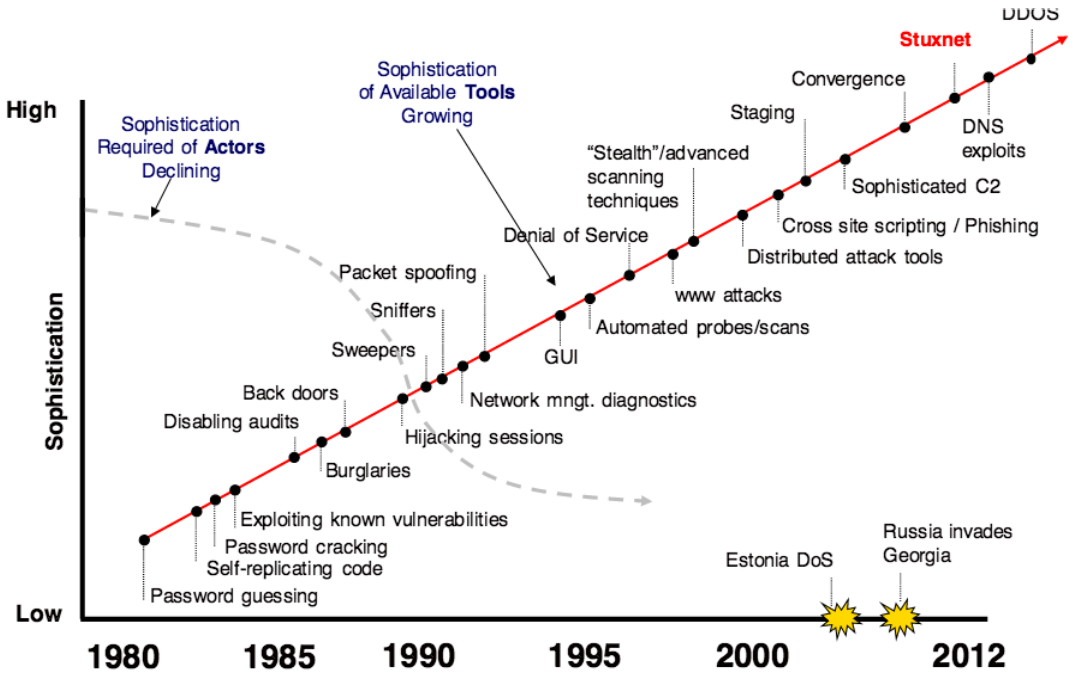

Figure 1. The Growth of the Cyber Threat[77]

[77] Source: "DHS_CSA_Cyber_Brief_AMSC_20140123_Willke.pdf," accessed March 10, 2016, http://infragardlouisiana.com/wp-content/uploads/2015/10/DHS_CSA_Cyber_Brief_AMSC_20140123_Willke.pdf.

III. SLTT THREAT ENVIRONMENT

Federal, state, and local governments occasionally face different forms and levels of cyber threats daily. A 2015 cybersecurity study, "State of Cybersecutrity in Local, State, and Federal Government," conducted by the Ponemon Institute, found that federal agencies rely more on intelligence sharing and are more effectively recruiting expert cyber personnel, and that federal agencies feel their cyber programs are in the late to mature stage while state officials feel their programs are in the early to middle stages of maturity. Over the past two-years, federal agencies have faced material security breaches every nine weeks, while state agencies faced them every 12 weeks. Lastly, state officials ranked their ability to prevent, detect, contain, and recover from a cyber-attack lower than federal officials. Both state and federal officials agreed that one of the top cybsersecurity objectives is to secure critical infrastructure assets.[78]

The Ponemon report points to the need for a more focused approach at the cybersecurity level. This approach needs to be scalable with the ability to share information efficiently from state to state. The information within the report identifies the need for an increased emphasis on ensuring SLTT entities develop a cybersecurity mission and implement strategies and policies designed to prevent, mitigate, and deter cyber threats targeted at state and local government computer networks. The remainder of the chapter looks at four areas of interest for every state's cyber security focus.

State and local government computer networks are continuously targeted by internal and external threats. This targeting has a direct impact on a company's intellectual property, security of critical infrastructure assets, and the protection of U.S. citizen's PPI.

A. STATE GOVERNMENT

The vulnerabilities of states can be seen in an August 2012 malicious email attack against the South Carolina Department of Revenue. An international hacker was able to

78 "State of Cybersecurity in Government FINAL," accessed March 3, 2016, https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6-2563enw.pdf.

crack into the state computer and gain access to "3.8 million tax returns, including Social Security numbers and bank account information, in what experts say is the biggest cyber-attack ever against a state government."[79] Cyber incidents involving PII can provide access to a treasure trove of information and lead to millions of records being stolen.[80]

Also in 2012, the CIO for the State of Utah, Mark VanOrden, stated "cybercriminals attack state computer at a rate of about 20 million times per day." This attack rate does not mean 20 million separate attacks but includes reconnaissance probes and computer automation. VanOrden went on to say, "every indication is that it (the attacks) will continue to accelerate."[81]

In December 2014, cyberterrorist hacked the Massachusetts State Police Department. The hackers gained access to the servers and locked out access to the police department. The criminals requested a $500 bitcoin ransom before releasing the server to the police department. DHS and the FBI were called in to support and identified a CryptoLocker malware had been present on the system since 2013. Only two options were available to the police department, pay the ransom or access the most recent backup of the database.[82] The department hired a contractor to restore the database and prevent future attacks. However, could government networks at the local level benefit from a state-level cybersecurity team or group who provides updates and monitors state computer networks to possible prevent or mitigate attacks of this nature?

Another example, in May 2013, the State of Washington reported a compromise of "up to 160,000 Social Security numbers and the names and driver's license numbers of

---

[79] Michael Isikoff, "One Email Exposes Millions of Personal Data Theft in South Carolina Cyber Attack," *NBC News*, November 20, 2012, http://investigations.nbcnews.com/_news/2012/11/20/15313720-one-email-exposes-millions-of-people-to-data-theft-in-south-carolina-cyberattack.

[80] U.S. Government Accountability Office, *Protecting Personally Identifiable Information* (GAO-08-343) (Washington, DC: U.S. Government Accountability Office, 2008), http://www.gao.gov/new.items/d08343.pdf

[81] "State Faces Millions of Cyber Attacks per Day, Department Head Says," accessed March 6, 2015, http://www.ksl.com/?nid=148&sid=24141005.

[82] "Cybersecurity: Police Department Pays Ransom after Hackers Encrypt Department's Data," April 6, 2015, http://www.homelandsecuritynewswire.com/dr20150406-police-department-pays-ransom-after-hackers-encrypt-department-s-data.

up to 1 million people, may have been compromised."[83] The potential breech actually occurred earlier in the year during the late February-early March timeframe. The breech is damaging because it involves so much PPI.[84]

"Breaches involving PII are hazardous to both individuals and organizations. Individual harms may include identity theft, embarrassment, or blackmail. Organizational harms may include a loss of public trust, legal liability, or remediation costs."[85] The impact of such a large amount of PPI stolen from the Department of Revenue may never been known. Moreover, in the 2012 Deloutte-NASCIO Cybersecurity Study,[86] state CIOs provided the following statistics:

> Government agencies have lost more than 94 million records of citizens since 2009, according to a recent Rapid7 report on the Data Breaches in the Government Sector.[87]
>
> The average cost per lost or breached record is $194 per the Ponemon Institute's 2011 Cost Data Breach Study.[88]

The NASCIO study also reported that 92% of state officials feel "cybersecurity is very important for the state and only 24% say they are very confident in protecting state's assets against external threats."[89] The reliance on computers within U.S. society will continue to increase. One way to increase confidence in the state's' ability to secure their networks is to ensure federal government strategies to protect the cyber domain include SLTT entities in the planning, development, and implementation of the various cybersecurity initiatives. The NASCIO study is also in favor of detailed plans for sharing

---

[83] "Washington State Courts Office Suffers Data Breach," May 9, 2013, http://www.govtech.com/security/Washington-State-Courts-Suffers-Data-Breach.html.

[84] Ibid.

[85] Government Accountability Office (GAO) Report 08–343, *Protecting Personally Identifiable Information*, January 2008, accessed on 12 Jan 2015; accessed from http://www.gao.gov/new.items/d08343.pdf.

[86] National Association of State Chief Information Officers (NASCIO), *2012 Deloitte-NASCIO Cybersecurity Study, State Governments at Risk: A Call for Collaboration and Compliance*.

[87] Rapid7, *Data Breaches in the Government Sector* (Boston, MA: Rapid7, 2012).

[88] Ponemon Institute, *2011 Cost of Data Breach Study: Global*.

[89] National Association of State Chief Information Officers (NASCIO), *2012 Deloitte-NASCIO Cybersecurity Study, State Governments at Risk: A Call for Collaboration and Compliance*, 3.

information and the implementation of security measures between federal and state information security organizations.

B. BANKING AND FINANCE

During an eight-month period starting in 2012 (October 2012–May 2013), several banks in Northeast Ohio (PNC, Key, Chase, and U.S. Bank) have been targeted by DDoS attacks that typically clog online and mobile access to accounts but also have the ability to compromise the banks' computer system.[90]

In December 2009, in the State of New York, Duanesburg Central School District, cyber criminals were able to transfer approximately $3 million dollars into overseas accounts.[91] However, most of the funds were able to be recovered with the help of the FBI. The intent, access, and vulnerability of financial and banking assets are constantly under attack, especially at the local and state level where their institutions are not afforded the same type of security mechanisms as the larger organizations.

Big banks and financial institutions like JPMorgan Chase & Co., Bank of America, Wells Fargo, Citigroup, PNC Financial Services Group and Bank of New York Melon have been consistently targeted over the years. As a result, they have bolstered their network defenses and have made it more difficult for cyber criminals to access their networks. Although, the threat is not gone, the banks are in a better position to prevent attacks and defend against the threat.

The adversary may now shift its attention to state, regional, and local (mid-tier) banks and financial institutions. The main attraction is a lack of security; the mid-tier banks lack the finances, IT, and personnel to ensure computer network protection and resilience.[92] The soft targets are easier to attack and with a possible lack of focus on

[90] Teresa Murray, "KeyCorp, U.S. Bank Websites Hit in the Latest Cyber Attack against Nation's Largest Banks," Cleveland.com, September 12, 2012, http://www.cleveland.com/business/index.ssf/2012/09/keycorp_us_bank_web_sites_hit.html.

[91] "Duanesburg Central School District," accessed January 15, 2013. http://duanesburg.org/district/news/0910/overview_onlinetheft.cfm.

[92] "Booz Allen Says Cyber Attacks Are the 'New Normal' for Financial Services Industry," accessed March 3, 2014, http://online.wsj.com/article/PR-CO-20131204-908341.html.

security; days, weeks, or months may go by before an intruder is detected inside the network.

C. INDUSTRIAL CONTROL SYSTEMS

Industrial control systems (ICS) are used to control critical information systems (power, water, natural gas, chemical, utility power, and energy systems). These systems are targets of opportunity from malicious actors because of the number of people that depend on the systems. Also, "on a daily basis, the U.S. is being targeted,"[93] said Sanaz Browarny, from DHS Intelligence & Analysis, during a panel discussion at GovSec Conference on April 4, 2012. Browarny went on to describe three forms of attacks, "There are … those being thrill-seeking 'garden-variety' hackers that target known vulnerabilities; secondly, the dangerous volley of viruses, worms and botnet attacks; and thirdly, 'nation-state actors' that have 'unlimited funding available' and conduct espionage as they establish a hidden presence on a sensitive network."[94]

Cyber operations as previously described provide critical insight into the tactics and techniques of a cyber-attack against critical infrastructure assets, specifically 23 natural gas companies. The attacker used malicious email links and file attachments that allowed access to company networks.[95] The cyber breach and the information stolen leave multiple compressor stations vulnerable to destruction. William Rush, with the Gas and Technology Institute, said, "Anyone can blow up a gas pipeline with dynamite. But with this stolen information, if I wanted to blow up not one, but 1,000 compressor stations, I could."[96] The seriousness of the breech can be enormous to the natural gas industry. The cyber criminals specifically targeted the pipeline operators. The information they wanted to access was specific to vulnerable compressors. U.S. networks are consistently probed for vulnerabilities and weaknesses. Former defense secretary Leon Panetta warned in October 2012, "that successful attacks have been made on

---

[93] "DHS: America's Water and Power Utilities under Daily Cyber-Attack, April 4, 2012, http://www.networkworld.com/news/2012/040412-dhs-cyberattack-257946.html.

[94] Ibid.

[95] Poeter, "50 Days of Mayhem: How LulzSec Changed Hacktivism Forever."

[96] Ibid.

computer control systems of American electricity and water plants and transportation systems."[97]

DHS reported a 52% increase in the number of attacks reported to the agency in 2012. Of the 198 attacks reported, the two most attacked sectors were energy (82) and water (29). In 2013, the total number of incidents had increased to 257. In 2014, the cyber incidents decreased by 12 to a total of 245. In 2014, the two most attacked sectors were critical manufacturing (159) and energy (79). Industrial control systems are countries' most critical computer networks.

In the 2012 report, DHS detailed several successful hacking attempts targeted at natural gas pipeline companies where the adversary had successfully exfiltrated data.[98] The attacks on the industrial control system is severe and getting costlier by the day. It is apparent that a stronger cyber defense shield is needed to protect American networks from malicious cyber actors. ICS networks are not alone in this increased cyber attacks by the adversary, colleges, and universities are also under increasing attacks.

Many states have identified their critical infrastructure assets and defined their points of criticality to ensure operational efficiency. The infrastructure assets are normally selected using criteria established DHS. The critical infrastructure assets are normally defined by physical and operational characteristics. The process of mapping the physical and operational touch points can be determined through certain criteria and asset interdependence. This process is tedious and time consuming but pays big dividends, as the final product provides a clear picture of what assets are important to the state. Now, once the assets are identified, how dependent are they on their computer networks or how vulnerable are they to cyber attacks?

Identifying the cyber fidelity of each asset is an even tougher process to accomplish. What is the cyber infrastructure of the physical assets? What is the structure

---

[97] Tom Simonite, "Old-Fashioned Control Systems Make U.S. Power Grids, Water Plants a Hacking Target," Security, October 12, 2012, http://securitynewsworld.wordpress.com/2012/10/15/old-fashioned-control-systems-make-u-s-power-grids-water-plants-a-hacking-target/.

[98] David Goldman, "Cyberattacks on Critical U.S. Infrastructure Rose 52% in 2012," *CNNMoney*, January 9, 2013, http://money.cnn.com/2013/01/09/technology/security/infrastructure-cyberattacks/index.html.

of the computer domain and networks? Is the network protected? What security protection standards are utilized by the infrastructure asset owners? Has the network been updated with the latest protection measures? These questions are critical in determining the cyber fidelity of the network and the security if the critical infrastructure asset.

D. EDUCATIONAL INSTITUTIONS

A prime target of cyber criminals is the open network contained within the U.S. universities and colleges digital infrastructure. A university campus is built for interconnectivity and access to the world. They are in the business of openness and communications, built on the idea of knowledge without walls or limitations; a free-flow of ideas and discussions, something for everyone, including the malicious cyber actor. Universities have hundreds of vulnerable access points for the malicious cyber actors to disguise their identity, deploy their tools, and launch larger attacks against banks, critical infrastructure, and industrial control systems.

Due to their mission to explore and connect their students to the world, universities and colleges provide an opportunity for cyber criminals to leverage their infrastructure to set up cyber attacks. Universities also have a tremendous amount of PII that can be stolen if not properly protected. The PII data is very attractive to cyber criminals, and if not properly protected, can be easily stolen.

The University of Wisconsin has reported as high as 90,000 to 100,000 cyber hacking attempts per day by state-sponsored actors from Russia, Vietnam, and China.[99] Although, it is noteworthy, the attacks appear to originate primarily from China; many cyber criminals are becoming increasingly adept at disguising their identity and location. A technology expert from Cornell University, speaking on recent cyber hacking attempts, said the "the attacks are increasing exponentially in attempts and sophistication."[100] At the University of Maryland, more than 100,000 attempted cyberattacks were reported on

[99] "U.S. Officials Say What's Been Stolen in Cyberattacks Sometimes Not Known," July 17, 2013, http://www.upi.com/Top_News/US/2013/07/17/US-research-universities-increasingly-targeted-by-cyberattacks/UPI-26641374065244/.

[100] Richard Pérez-peña, "Universities Face a Rising Barrage of Cyberattacks," *The New York Times*, July 16, 2013, http://www.nytimes.com/2013/07/17/education/barrage-of-cyberattacks-challenges-campus-culture.html.

July 25, 2013, by early afternoon.[101] Federal agencies have an important role in supporting colleges and universities.

On February 20, 2014, William Loh, President, University of Maryland, announced in a statement, "The personal information of more than 309,000 students, staff and alumni of the university was compromised in a sophisticated cyber-attack … I am very sorry." The cyber-attack stole students' PPI to include student identification numbers, social security numbers, and birth dates. The adversary was very cunning and was able to access the university's computer network even though it was protected by "multi-layered security defenses."[102]

In April 2015, the University of California at Berkeley was targeted by a cyber-attack where hackers were able to steal the social security numbers from 260 former and current undergraduate students and 290 parents and family members of the students. One month later in May, Penn State University was hacked and 18,000 social security numbers and personal information was exposed and exfiltrated from university networks.[103]

The NSA and DHS under a jointly sponsored program, have identified National Centers of Academic Excellence (CAE) in IA (Information Assurance) Education (IAE), the program supports colleges and universities by promoting higher education and research in IA. A wealth of information and research (technology, nuclear, nautical, aeronautic, and military, computer, etc.) is held and analyzed at these institutions of higher learning. It should be of utmost importance to keep this information secured from cyber criminals or state-sponsored actors.[104]

---

[101] "University of Maryland Researchers Fend off Steady Cyber Risks," accessed January 17, 2014, http://www.diamondbackonline.com/news/campus/article_4158cd62-fa5c-11e2-afd7-0019bb30f31a.html.

[102] Colin Campbell, "More than 309,000 Identities Exposed in University of Maryland Cyberattack," *Baltimoresun.com*, accessed March 2, 2014, http://www.baltimoresun.com/news/maryland/bs-md-university-of-maryland-data-breach-20140219,0,2321285.story.

[103] Amir Nasr, "Universities Increasingly Falling Victim to Cyberattacks," *Morning Consult*, July 11, 2015, http://morningconsult.com/2015/07/universities-increasingly-falling-victim-to-cyberattacks/.

[104] "National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD)," accessed April 12, 2016, https://www.nsa.gov/ia/academic_outreach/nat_cae/.

E. PERSONABLE IDENTIFIABLE INFORMATION

In the 2012 Deloutte-NASCIO Cybersecurity Study,[105] state CIOs provided the following information on the value of stolen PII. In a targeted attack against the Department of Revenue, a large amount of PII was stolen and NASIO provided the following statistics:

> Government agencies have lost more than 94 million records of citizens since 2009, according to a recent Rapid7 report on the Data Breaches in the Government Sector.[106]
>
> The average cost per lost or breached record is $194 per the Ponemon Institute's 2011 Cost Data Breach Study.[107]

One area of increasing concern has been the introduction of the Affordable Care Act, which opened its government marketplace on October 1, 2013. The initial website difficulties identified several security network vulnerabilities that appear to be associated with the 14 state marketplace websites.[108] Also, minor cyber breaches were identified in Vermont, South Carolina, and North Carolina.[109] DHS's Cybersecurity and Communications division reported in November 2013 that the Healthcare.gov site had been targeted 16 times by cyber attacks in various forms to include at least one unsuccessful DDoS attack.[110] As more and more individuals sign up for the health insurance, the need for increased security to protect personal and health data will also increase at both the state and federal level. As a result, attempted PII data breaches will

---

[105] National Association of State Chief Information Officers (NASCIO), *2012 Deloitte-NASCIO Cybersecurity Study, State Governments at Risk: A Call for Collaboration and Compliance*, Executive Summary.

[106] Rapid7, *Data Breaches in the Government Sector*.

[107] Ponemon Institute, *2011 Cost of Data Breach Study: Global*.

[108] Elizabeth Harrington, "Expert: Healthcare.gov Security Risks Even Worse After 'Fix,'" *Washington Free Beacon*, accessed January 21, 2014, http://freebeacon.com/expert-healthcare-gov-security-risks-even-worse-after-fix/.

[109] "State Confirms Health website Security Breach," accessed January 21, 2014, http://www.burlingtonfreepress.com/article/20131122/NEWS03/311220030/State-confirms-health-website-security-breach.

[110] Michael Isikoff, "HealthCare.gov Targeted 'about 16 Times' by Cyberattacks, DHS Official Says," *NBC News*, November 13, 2013, http://investigations.nbcnews.com/_news/2013/11/13/21440068-healthcaregov-targeted-about-16-times-by-cyberattacks-dhs-official-says.

probably become increasingly attractive to cyber criminals who target PII for personal, financial, and network intrusion purposes.

In closing, research indicates that cyber attacks will continue to grow at the state and federal level. The U.S. computer network is a target-of-opportunity for state-actors and independent cyber criminals. Targeted attacks will continue to increase in the state government, education, industrial control systems, and PII areas. Many industries also provide prime targets, as the medical, defense, energy, financial, and government networks continue to be under attack by adversaries. A concerted and focused effort is needed prevent attacks posed by persistent cyber threats, to protect PII, financial data, control systems, and government networks. The failure to address this issue now leaves the United States vulnerable to the loss of revenue, operational interruptions, identity theft, loss of intellectual property, and unforeseen consequences.

This chapter discussed the current cyber threat to the nation, to SLTT entities, and the cyber security policies and laws that affect the protection of federal SLTT governments. The impact of the threat on national security and the absence of overarching cyber security law directives, EOs, and memorandums of agreement to protect U.S. computer networks is considerable. The next chapter focuses on the response to the threat.

IV. THE RESPONSE TO THE THREAT

The rise in cyber attacks on government, military, public and private, state and local networks shows that the threat to U.S. computer networks is real, consistently increasing, and evolving in complexity. In 2013, DHS United States Computer Emergency Readiness Team (US-CERT) received 46,160 notifications of cyber incidents from 24 government agencies. The information reported by government agencies has increased over the past two years by 32%.[111] DHS's Industrial Control Systems-CERT (ICS-CERT) received 257 notifications of cyber incidents from critical infrastructure organizations throughout the nation. The US-CERT and ICS-CERT offer tools and services to federal department and agencies, critical infrastructure asset owners, state and local governments, and private sector stakeholders to assist with cyber incident protection, response, and mitigation. This daunting task falls under the authority of the NCCIC. The NCCIC received over 220,000 total cybersecurity and communications incidents in 2013.[112] "The NCCIC is a 24x7 cyber situational awareness, incident response, and management center. The Centers mission is to reduce the likelihood and severity of cyber and communication incidents as it relates to the Nation's information technology and communication networks."[113] The NCCIC is the federal government's first-line of defense to protect .gov domain and its departments and agencies against cyber incidents. However, the agency is not alone. Several agencies within the cyber environment work together in this task to protect military and government networks and information. Table 1 identifies the six organizations and their mission. Each organization has a specific mission and capabilities. The organizations share information and coordinate cyber prevention, detection, mitigation, and recovery efforts. This

[111] U.S. Government Accountability Office, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent* (GAO-14-34) (Washington, DC: U.S. Government Accountability Office, 2013), http://www.gao.gov/assets/660/659572.pdf.

[112] National Cybersecurity and Communications Integration Center, *ICS-CERT Year in Review* (Washington, DC: Department of Homeland Security, 2013), https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_In_Review_FY2013_Final.pdf.

[113] "About the National Cybersecurity & Communications Integration Center," accessed October 16, 2014, http://www.dhs.gov/about-national-cybersecurity-communications-integration-center.

collaboration between organizations is very dynamic and provides the information-sharing foundation design to protect critical infrastructure, military, and U.S. government departments and agencies (D/A) networks.

Table 1. United States Federal Cyber Centers[114]

Agency	Organization	Mission
DHS / NCCIC – (US-CERT) – (ICS-CERT)	National Cybersecurity & Communications Integration Center	Serves as a centralized location where operational elements involved in cybersecurity and communications reliance are coordinated and integrated.
DIA / IC-SCC	Intelligence Community (IC) – Security Coordination Center	Provides vulnerability management notification and status reporting for the IC
FBI / NCIJTF	National Cyber Investigative Joint Task Force	Conducts Law Enforcement/ Counter-Terrorism cyber-related investigations and response to counterintelligence threats
DOD / DC3	DOD Defense Cyber Crime Center	Serves as focal point for the Defense Industrial Base (DIB)
DOD / U. S. Cyber Command (USCC)	USCC Joint Operations Center	Develops strategic framework for GIG operations.

(continued on next page)

[114] Data from "National Cybersecurity Center Policy Capture," accessed December 12, 2012, http://www.whitehouse.gov/files/documents/cyber/CybersecurityCentersGraphic.pdf.

Table 1 (continued from previous page)

Agency	Organization	Mission
NSA / NTOC	National Threat Operations Center	Facilitates and coordinates identification and development of countermeasures

As the nation goes about trying to protect its information, a key concern within the cyber community at the state level is deciding the best way to protect the SLTT organizations. The Multi-State Information Sharing and Analysis Center (MS-ISAC) performs a similar function as the six previously mentioned cyber centers with its customers being state and local entities. The MS-ISAC is a voluntary and collaborative partnership with the DHS's National Cyber Security Division to provide key resources for "cyber threat prevention, protection, response and recovery to the nation's state, local, territorial and tribal governments."[115] The MS-ISAC serves as a key operational conduit between the federal government and SLTT governments. MS-ISAC operates a 24x7x365 operations center providing real-time network monitoring, early warning, vulnerability identification and mitigation, and incident response for the SLTT community.[116] The MS-ISAC has the ability to contact its members and correlate cyber attacks between members and organizations. The center also provides cyber advisories and threat reporting it receives from the NCCIC. The MS-ISAC was established in 2003. The connection between the federal cyber center and the state and local governments through the MS-ISAC has consistently grown from an information-sharing and collaboration aspect. The next section looks at policies and laws at the federal and state government levels designed to protect U.S. computer networks.

[115] Multi-State Information Sharing & Analysis Center, *MS-ISAC Membership Overview* (East Greenbush, NY: Center for Internet Security, 2012), http://msisac.cisecurity.org/about/documents/MS-ISACMembershipOverview2012.pdf.

[116] "Multi-State Information Sharing and Analysis Center," accessed February 13, 2014, http://msisac.cisecurity.org/.

A. CYBERSECURITY POLICY

The Cybersecurity Act of 2012 was introduced to Congress in February of that year. Congress was unwilling to pass the bill in 2012. However, pressure mounted as DDoS attacks hit major banks in 2012. In 2013, Apple, Facebook, and Twitter became high-profile victims of hacking. In 2014, Anonymous hacked the North Korean government and defaced Israeli websites. Also, in 2014, the Heartbleed bug exposed 65% of all internet traffic to data leaks. Finally, in 2015, the Office of Personnel Management (OPM) (more than 21 million were affected by the data breach[117]) and Sony Pictures Entertainment breach, and subsequent canceling of the planned release of the movie "The Interview," appeared to be the tipping point to enable Congress to move and pass this legislation.

President Obama signed the Cybersecurity Act of 2015 into law on December 18, 2015. In summary, the Act requires DHS to establish a portal for receiving cyber threat indicators from the private sector and sharing them with both public and private sector entities. As an incentive, the Act "provides targeted liability protection to companies that share cyber threat indicators with DHS."[118] The bill limits the purpose for which the "government may use shared information to certain cybersecurity purposes."[119] The bill also requires "two layers of privacy protections: companies must remove personal information before sharing cyber threat indicators"[120] with DHS, and DHS must implement privacy reviews of all indicators it receives. The bill also mandates federal departments and agencies deploy EINSTEIN capabilities within the next year. The bill gives increased authority to DHS and provides protections and incentives for private industry.

For the purposes of this thesis, the Director of National Intelligence (DNI) and the DHS Secretary are responsible for developing procedures to share cybersecurity threat

---

[117] "OPM Notifies 3.7 Million Cyber Attack Victims," October 28, 2015, http://federalnewsradio.com/cybersecurity/2015/10/opm-notifies-3-7-million-cyber-attack-victims-about-data-protection-services/.

[118] "Senate Report 114–32, United States Senate S.754—Cybersecurity Information Sharing Act of 2015," accessed December 28, 2015, https://www.congress.gov/bill/114th-congress/senate-bill/754.

[119] Ibid.

[120] Ibid.

information with state, tribal, and local governments. This requirement provides direct support to SLTT entities and allows for increased emphasis on sharing information to protect critical government computer systems.

B. DHS AND DOD CYBER AGREEMENT

In 2010, current Secretary of Homeland Security Janet Napolitano and Secretary of Defense Robert Gates signed a memorandum of agreement (MOA) on cybersecurity "outlining the personnel, tools and facilities the two departments will share to improve collaboration on cyber activities."[121] In a joint statement, the Secretaries stated, "We will improve economy and efficiency by better leveraging vital technologies and personnel to serve both departments' missions in full adherence to U.S. laws and regulation. This memorandum of agreement furthers our strong commitment to protecting civil liberties and privacy."[122] This cyber partnership has provided joint opportunities for collaboration amongst the agencies in support of cyber defense. An example is the Joint Cybersecurity Services Pilot, a program designed to use NSA tools and capabilities to protect defense industrial base (DIB) computer networks. The program works with internet service providers to provide protection against "Domain Name System (DNS) sink holing, which involves blocking DNS traffic to malicious domains, and 2) email filtering that includes quarantining infected messages."[123] The two cyber-attack vectors are used by adversaries as tools to penetrate U.S. computer networks with viruses and remove data from computer databases. In January 2012, DOD transferred the operational control of this program to DHS.[124]

The partnership between the two agencies (DOD and DHS) has provided DHS the opportunity to offer this voluntary program to companies within all 17 critical infrastructure sectors. The program, which began as a proof-of-concept, has become a

---

[121] "Defense and DHS Reach Cybersecurity Compromise," accessed January 31, 2014, http://www.nextgov.com/cybersecurity/2010/10/defense-and-dhs-reach-cybersecurity-compromise/47758/.

[122] Ibid.

[123] "DHS Teams with DOD on Cybersecurity Project with Industry," accessed January 31, 2014, http://www.infosecurity-magazine.com/view/23348/dhs-teams-with-dod-on-cybersecurity-project-with-industry/.

[124] Ibid.

partnership model between DOD, DHS, and private industry. The goal of the program is to share sensitive indicators and signatures and to utilize internet service providers to share cyber defense information with private industry. The DIB Opt-In Pilot program was renamed under DHS to the Enhanced Cybersecurity Service (ECS) program.[125]

The ECS program has been under DHS operational control since 2013. The program provides a unique set of data that can be provided to commercial service providers (AT&T, CenturyLink, Lockheed Martin, and Verizon). The program currently offers three types of services: DNS sinkholing, email filtering, and Netflow analysis).[126] During an interview in October 2014, Dr. Andy Ozment, the DHS assistant secretary of the Office of Cybersecurity and Communications said, "the data [from the ECS program] is unique … but a challenge here is the data doesn't lend itself to easy comparison." He went on to say, "We think there is value in using this information to protect companies."[127]

C. DHS ENGAGEMENT

The role of DHS in the defense of the nation's cyber domain can be found in the following laws and presidential directives: Homeland Security Act of 2002 and Homeland Security Directive 7 (HSPD-7) tasked the Secretary of Homeland Security to:

- Coordinate the protection of critical infrastructure and key resources (CIKR) throughout the nation.
- Coordinate the protection efforts for the IT, telecommunications, and emergency services sectors (among others).
- Identify one agency as the primary government representative for cyberspace.
- Provide cybersecurity assistance to state and local government entities.

---

[125] Department of Homeland Security, *Enhanced Cybersecurity Services* (Washington, DC: Department of Homeland Security, 2016), https://www.dhs.gov/sites/default/files/publications/ECS-Fact-Sheet_no%20stats_02.2016.pdf.

[126] Ibid.

[127] Jason Miller, Federal News Radio, *DHS says cyber initiatives healthy and growing*, October 9, 2014, accessed on 15 October 2014, accessed from http://federalnewsradio.com/technology/2014/10/dhs-says-cyber-initiatives-healthy-and-growing/.

"HSPD 5 establishes DHS's incident management responsibilities in the event of a terrorist attack or presidential major disaster or emergency declaration, while HSPD-7, requires DHS to maintain an organization to serve as the focal point for cybersecurity coordination among Federal departments and agencies, State and local governments, the private sector, academia, and international organization."[128]

D. EXECUTIVE ORDERS AND DIRECTIVES

Cybersecurity EO 13636 and PPD-21 leads the nation's efforts to secure the .gov domain to include securing critical infrastructure networks by providing assistance to private sector owners and operators.[129] DHS plays a critical role along with public private partnership to prevent, respond, and mitigate cyber attacks.[130] EO 13636 works in conjunction with PPD-21, which replaces HSPD-7.[131]

EO 13636 provides for the following:

- Technology-neutral voluntary cybersecurity framework
- Adoption of cybersecurity best practices
- Increased cyber threat information sharing
- Incorporation of strong privacy and civil liberties protections[132]

PPD-21 provides for the following:

- Providing both physical and cyber infrastructure

---

[128] Ibid.

[129] "Secure Cyber Networks," accessed January 31, 2014, https://www.dhs.gov/secure-cyber-networks.

[130] Department of Homeland Security, *Fact Sheet: EO 13636 Improving Critical Infrastructure Cybersecurity and PPD 21 Critical Infrastructure Security and Resilience* (Washington, DC: Department of Homeland Security, 2013), http://www.dhs.gov/publication/fact-sheet-eo-13636-improving-critical-infrastructure-cybersecurity-and-ppd-21-critical.

[131] Critical Infrastructure: "As used in EO 13636, means systems and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." "Improving Critical Infrastructure Cybersecurity," accessed February 1, 2014, https://www.federalregister.gov/articles/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity.

[132] Department of Homeland Security, *Fact Sheet: EO 13636 Improving Critical Infrastructure Cybersecurity and PPD 21 Critical Infrastructure Security and Resilience*.

- Understanding infrastructure failures
- Maturing the public-private partnership
- Updating the National Infrastructure Protection Plan
- Developing a comprehensive research and development plan[133]

The combined implementation of the EO 13636 and PPD-21 is designed to secure critical infrastructure networks by identification, protection, detection, recovery, and mitigation through network security measures. The orders established timelines for implementation:

- Expanded sharing of cybersecurity information by June 12, 2013
- Establishment of a cybersecurity framework by October 10, 2013
- Use of a risk-based approach to identify critical infrastructure with a cybersecurity impact could result in catastrophic damage by July 12, 2013[134]

This chapter has discussed the national response to the cyber threat. The cybersecurity strategies, policies, EOs and laws are primarily designed to support information sharing at the federal level and between public and private industry partners. The operational framework provides a standard that can be used across the cyber landscape to ensure specific guidelines are followed throughout the cyber community. However, one missing area in the strategy is the protection of SLTT government networks. How do the SLTT computer networks fit into the cybersecurity protection plan for the country? The next chapter takes a closer look at the SLTT cyber threat.

---

[133] Ibid.

[134] "Executive Order and Policy Directive Promotes Cybersecurity Cooperation and Intelligence Sharing," accessed February 1, 2014, http://www.privsecblog.com/2013/02/articles/main-topics/data-breach-security/executive-order-and-policy-directive-promotes-cybersecurity-cooperation-and-intelligence-sharing/.

V. SLTT CYBER COLLABORATION

> The sophistication of cybercrime TTPs (Tactics, Techniques, and Procedures) is highly likely to continue to increase in 2014, with enhanced malware and more sophisticated delivery techniques and that financially-motivated malware is likely to continue to dominate the SLTT threat picture.
>
> ~ Center for Internet Security

Many areas of the cyber domain are under attack: critical infrastructure, electrical grids, banks, business, government, colleges and universities and PPI (identity theft, medical records, credit card theft, child exploitation, etc.) of American citizens. As the country and the world moves towards an increasingly digitized future, state and local governments have become increasingly dependent upon computerized networks, digital storage, internet communications, and automation of critical infrastructure services during the daily business cycle. Since their databases and networks hold some much of the citizens' PII and because they do not have the cyber protection resources afforded to the federal government, they are rich targets of opportunity by malicious cyber actors.

Maryland Governor Martin O'Malley, during a panel discussion at the 2011 National Governors Association (NGA) meeting said, "Cyber-attacks on state and federal databases are "one of the nation's greatest emerging threats." Governor O'Malley voices a concern shared by many governors and state CIOs, in that the cyber threat to SLTT entities is a top priority within their administration.

The threats to state and local governments can be directly related to homeland security cyber vulnerabilities. This chapter focuses on the collaboration efforts between federal and state governments to protect and secure computer networks at the state and local level.

A. BUILDING PARTNERSHIPS

DHS is chartered to provide support to SLTT entities. As a result, they have effectively set up a partnership environment connecting the federal government with state and local governments through the use of voluntary councils.

(1) The Critical Infrastructure Partnership Advisory Council

The (CIPAC) was established by DHS to "facilitate effective coordination between federal infrastructure protection programs with the infrastructure protection activities of the private sector and of state, local, territorial and tribal governments."[135] It brings together federal and SLTT entities from across the nation to partner to discuss the protection of critical infrastructure assets and key resources.[136]

The CIPAC was chartered and signed by DHS Secretary Janet Napolitano in March 2010 under the authority of the Homeland Security Act of 2002. The CIKR sector representatives were established by HSPD-7.[137] The council organizes strategies for both physical and cyber infrastructure protection efforts as they support CIKR resources. Since its organization in 2010, only 30 states currently have representatives on the council.[138] Does any correlation exist between a lack of organizational effectiveness and number of states participating? What is the reason for the other 20 states' lack of representation on the council?

---

[135] "Critical Infrastructure Partnership Advisory Council," accessed February 5, 2014, http://www.dhs.gov/critical-infrastructure-partnership-advisory-council.

[136] Department of Homeland Security, *Critical Infrastructure Protection Advisory Council (CIPAC) Charter* (Washington, DC: Department of Homeland Security, 2010), http://www.dhs.gov/xlibrary/assets/cipac/cipac_charter.pdf.

[137] Ibid.

[138] "State, Local, Tribal, and Territorial Government Coordinating Council: Charter and Membership," April 13, 2016, https://www.dhs.gov/slttgcc-charter-and-membership.

(2) The Information Technology Sector Coordination Council

The IT-SCC was established in January 2006 to bring together companies, associations, and other key IT sector participants to coordinate infrastructure protection, response, and recovery within this sector.[139]

(3) The IT-Government Coordinating Council

The IT-GCC also brings together federal and SLTT entities from across the nation that focus on the strategies and initiatives to help protect the technology associated with critical infrastructure assets.[140] Together, the government coordination councils bring together over 200 companies from the public and private sector and over 11 federal government partners to meet the needs of stakeholders (business, citizens, companies, etc.) throughout the country.[141] The IT-SCC and IT-GCC are policy councils that provide strategies aimed to increase collaboration and information sharing between agencies.

(4) The Cybersecurity Partner Local Access Plan

The CPLAP leverages state fusion centers capabilities as platforms to facilitate classified cybersecurity information sharing.[142] The program, which began as a pilot in March 2010, equips fusion centers with the ability to pass secret-level information on cyber threats to state and local government and industry partners who have security clearances.[143]

The CPLAP program uses existing fusion center infrastructure to law enforcement or homeland security partners to provide higher level of information to state and local, critical infrastructure, and law enforcement personnel who are classified at a certain security level. Classified information forwarded to fusion centers can also be downgraded

---

[139] "ITSCC Overview," accessed March 17, 2014, http://www.it-scc.org/about.html. .

[140] "DHS State Government Offerings, Products, and Services," accessed February 9, 2014, http://www.dhs.gov/sites/default/files/publications/DHS%20State%20Resources_0.pdf.

[141] "Specific Plan 201," accessed February 11, 2014, http://www.it-scc.org/documents/itscc/nipp-ssp-information-tech-2010.pdf.

[142] "DHS State Government Offerings, Products, and Services."

[143] Ben Bain, "DHS, Industry to Try Fusion Centers for Classified Data Swap," Federal Computer Week, March 16, 2010, https://fcw.com/articles/2010/03/16/web-cyber-threat-fusion-center.aspx.

through the use of tear-line information and provided to a larger audience. Tear-line information allows for intelligence to be downgraded to ensure the security of sources and methods.

The four programs discussed in this section are targeted to benefit information sharing between federal, and state and local entities. However, none of these programs focuses primarily on protecting SLTT networks. The information-sharing process is being discussed at the strategic level between senior executives. Most states have small IT organizations with limited security expertise. Information-sharing strategies are always welcomed but to deter the threat, the sharing process will need to be migrated from a theory to an operational plan.

B. GOVERNMENT INFORMATION SHARING

As discussed in Chapter II, the federal government has established federal cyber centers to assist in the protection of military, federal and critical infrastructure networks. Several programs and organization at the federal and state-level provide support to SLTT entities.

1. Multi-State Information Sharing and Analysis Center (MS-ISAC)

The MS-ISAC is a voluntary and collaborative partnership with DHS's NCCIC to provide key resources for "cyber threat prevention, protection, response and recovery to the nation's state, local, territorial and tribal governments."[144] The NCCIC is a division of DHS's NPPD and operates "at the intersection of the private sector, civilian, law enforcement, intelligence, and defense communities."[145] The NCCIC collaborates with SLTT governments through its close relationship with the MS-ISAC. MS-ISAC has a liaison representative on the NCCIC operations center floor. This representative ensures close collaboration between the NCCIC operations center and the MS-ISAC security operations center (SOC) located in East Greenbush, New York.[146]

---

[144] Multi-State Information Sharing & Analysis Center, *MS-ISAC Membership Overview*.

[145] Ibid.

[146] Ibid.

The MS-ISAC has membership representation from all 50 states. The state representatives are normally chief cyber security officers, homeland security personnel, or law enforcement professionals. From a state perspective, the MS-ISAC has a representative from all 50 state capital cities. Many states also have representatives from within their major city locations. The MS-ISAC has representatives in U.S. territories (American Samoa, Guam, Puerto Rico, and U.S. Virgin Islands) and tribal nations (Gila River Indian Community, AZ, Morongo Band of Mission Indians, CA, Mohegan Tribe, CT, and Choctaw Nation, OK) in an attempt to expand their outreach throughout all areas of SLTT governments[147]

NCCIC's relationship with the federal cyber centers and its unique relationship with the MS-ISAC allows for the collaboration of cyber threats, warnings, advisories, vulnerabilities, mitigation, and incident response capabilities at a high level of collaboration within the cyber domain. However, can the cyber support be more efficient, incorporate a more targeted threat response, or be developed to allow SLTT governments to implement the cyber procedures received from federal government partners?

The MS-ISAC partnership with SLTT governments is important not only in the security of their networks, but it also has mutual value to federal partners when analytical collaboration provides actionable indicators and targeted analysis leads to the building of signatures and countermeasures to deter or prevent future attacks and threats. The collaboration process is great but the process falls short if the SLTT government stakeholders do not have the capability to process the data or implement the recommended cyber procedures.

2. Cyber Security Advisor Program (CSA)

"CSAs act as principal field liaisons in cybersecurity and provide a Federal resource to regions, communities, and businesses. Equally important is their role in supporting cybersecurity risk management efforts at the State and local homeland security initiatives. Their primary goal is to assist the Nation's critical infrastructure and

[147] "Multi-State Information Sharing and Analysis Center."

key resources (CI/KR)."[148] The program is run by DHS' Cybersecurity and Communications (CS&C) Strategic Engagement and Cyber Infrastructure Resilience (SECIR) Division and is structured in the same manner as the Protective Security Advisor (PSA) program run by DHS's Infrastructure Protection Division. The CSA program focuses on cyber security while the PSA program focuses on physical security. The CSAs projects the capabilities of the NCCIC to be extended to state and local governments.[149] The primary goal of this program is to bolster the cybersecurity infrastructure of CIKR assets within specific Federal Emergency Management Agency (FEMA) regions (shown in Figure 2).

Figure 2. Fusion Center Regional Areas[150]

[148] "Cybersecurity and Communications (CS&C)," accessed February 13, 2014, https://www.dhs.gov/xlibrary/assets/pso_cat_csc.pdf.

[149] Office of Cybersecurity and Communications, *CSA Security Advisor Initiative Pre-Decisional Implementation Plan* (Washington, DC: Department of Homeland Security, 2014), 5.

[150] Source: "Regional Contacts," accessed April 8, 2013, http://www.greatdreams.com/political/RegionalContacts.jpg.

Currently, four CSAs are deployed within the FEMA regions. The goal was to have one CSA deployed to each region, for a total of 10, by the end of 2015. CSAs work closely with CISOs. They serve as an additional capability within fusion centers and within state and local emergency operations centers (EOCs). In addition, they are a conduit between CS&C and the SLTT and private industry.[151] CSAs normally perform a particular, non-operational role when notified and directed by federal officials and at the request of state, local, and private sector emergency managers. From a cyber notification and response perspective, the CSAs do not perform response actions directly. They normally provide assistance with on-site and front-line damage control, notification and outreach to the national sector, on-site command and control of cyber first responders, and on-site contingency plan activation, monitoring, and oversight.[152] Cyber security advisors are deployed from the Cyber Security Evaluation Program (CSEP).[153] The CSEP performs cyber resilience reviews (CRRs) that measure adoption of maturity aspects of cybersecurity risk management using a common, capability-based framework.[154] This process improvement model was developed by Carnegie Mellon University's Software Engineering Institute for managing operational resilience.

CSAs are primarily advisors from the federal government to facilitate cybersecurity assistance as needed to state and local governments. The role of the CSA and their relationship with CISOs and CIOs provide needed support to protecting cyber infrastructure at the state and local level. However, can the role of the CSA be bolstered to provide hands-on operational cyber support? The CSA's role as a facilitator and senior representative interacting with CISOs and CIOs are surely needed. Moreover, an additional responsibility to provide direct cyber operational support will also increase efficiency and provide much needed resource for cyber threat prevention, protection, response, and recovery to the nation's SLTT governments.

---

[151] Office of Cybersecurity and Communications, *CSA Security Advisor Initiative Pre-Decisional Implementation Plan*, 6.

[152] Ibid., 7.

[153] Ibid., 4.

[154] "DHS State Government Offerings, Products, and Services."

3. National Guard

The National Defense Authorization Act signed in December 2013 and the Cyber Warrior Act of 2013 provide for the use of the National Guard in a cyber defense role in support of the states in case of a cyber disaster. The State of Washington was one of the first to embrace this initiative by using the guard for cyber emergency "planning and to search for vulnerabilities in its state networks through 'red team' exercises."[155] High-tech companies in Washington like Google, Microsoft, Cisco, Hewlett-Packard, and others provided the state with a wealth of Guard soldiers working in technology companies every day. They were current in the cyber threat and the technology used to prevent and deter cyber attacks. The guard provides a unique military prospective on cybersecurity with possible direct connections to training and capabilities through the NSA and U.S. Cyber Command (USCC).

In March 2013, a group of eight senators introduced a bill that would establish National Guard led, cybersecurity civil support teams, under the direction of the governor of the state. The teams could be activated in response to a major cyber-attack.[156] When discussed with General Keith B. Alexander, Director of the NSA and Commander of USCC, General Alexander responded, "we are actively working this issue with the Guard, he went on to explain how he had presented the idea to all of the adjutant generals from all the states and walked them through the process of standards and training."[157] The ability to leverage the experience of IT professionals at a fairly low-cost is a very attractive option in the fight against malicious cyber actors and criminals.

---

[155] The Pew Charitable Trusts State and Consumer Initiatives Site Map Search, "The National Guard Takes on Hackers," *The Pew Charitable Trusts*, January 28, 2014, http://www.pewstates.org/projects/stateline/headlines/the-national-guard-takes-on-hackers-85899535957.

[156] Mickey McCarter, "Senators Seek National Guard Cybersecurity Civil Support Teams," Homeland Security Today, March 27, 2013, http://www.hstoday.us/briefings/daily-news-analysis/single-article/senators-seek-national-guard-cybersecurity-civil-support-teams/8461dd77befa9b1506273a976c5c2b15.html.

[157] Ibid.

In addition to the state of Washington, five other states (Missouri, Maryland, Delaware, Utah, and Rhode Island) have all established cyber response teams.[158] The states believe Guard mobilization against cyber attacks can play a critical role in the defense of state and local networks. This initiative gained momentum during 2013–14 due to the lack of movement by Congress to pass a comprehensive cybersecurity bill that will protect both federal and state and local networks. As stated by Colorado Governor (John Hickenlooper (D), during his "State of the States" speech at the National Governors Association in January 2014, "While the federal government seeks to clarify how it will work with private sector and states to better secure cyberspace, states are already moving forward to develop and implement new cyber policies to protect their economies and ensure public safety."[159]

The National Guard has the potential to provide a low-cost and effective cyber threat, mitigation, and recovery alternative for the nation's SLTT governments. This initiative can leverage the cyber capabilities of DHS and the FBI possibly to form a team of cyber defenders that can provide targeted cyber support and mutual value to state and local government, as well as value to the federal government.

In closing, it should be noted, DHS has a three page list of products and services available to SLTT entities. The services provided specific information on collaboration, information sharing, classified data sharing, evaluations and assessments, software assurance, and exercises and training to name a few. The services are mostly free of charge and are provided to ensure cybersecurity information is forwarded and collaborated at all levels of government.

This chapter examined the cyber threat and the seriousness of the threat to state and local governments. It discussed the various programs, partnerships, and the accompanying policies that allow federal government assets, information, and capabilities to be leveraged by SLTT governments. A variety of programs are targeted at

---

[158] Kevin McCaney, "Got a Cyber Emergency? Call out the National Guard," Defense Systems, January 30, 2014, http://defensesystems.com/articles/2014/01/30/national-guard-cyber-response.aspx.

[159] Melissa Maynard, "The National Guard Takes On Hackers," STATELINE, January 28, 2014, http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2014/01/28/the-national-guard-takes-on-hackers

different aspects of the problem set (securing SLTT government networks). In conclusion, the previous example demonstrates the variety of programs available to SLTT entities, and as stated section 1, only 24% of state CIOs are very confident in protecting states' assets against external threats, even with all the information-sharing initiatives and tools provided by the federal government.

Chapter V looks at state and local fusion centers and examined if fusion centers are a viable option to protect SLTT computer networks.

VI. FUSION CENTERS: MISSION AND OPPORTUNITY

As discuss earlier, fusion centers are designed to receive, analyze, disseminate, and gather information. Chapter four documents visits to fusion centers in Maryland and San Francisco and discusses the mission of the Delaware and Virginia fusion centers. The visits were designed as an information gathering process. An opportunity to review firsthand the mission of the fusion centers and ascertain through a review of the operations tempo, operational procedures, operational relationships between the federal and local governments, mission delegation, governing documents, and overall mission process. A review of this material also provides an assessment of the fusion centers' ability to absorb an additional cybersecurity mission. The fusion center information that follows is based upon the author's visit to the centers.

A. THE HISTORY OF FUSION CENTERS

The Homeland Security Act of 2002 created DHS. The President was required to "implement procedures for Federal agencies to share classified and unclassified homeland security information with appropriate State and local personnel (including private-sector entities)."[160] Fusion centers were designed to serve as a primary state and local information-sharing organization between the federal government, state and local, and public and private sector.[161]

In 2004, the 9/11 Commission Report was released. The Commission highlighted the failure of public officials to "connect the dots." The inability of the federal and state intelligence and law enforcement officials to identify and prevent the threat was highly

[160] National Infrastructure Advisory Council, *Intelligence Information Sharing, Final Report and Recommendations* (Washington, DC: Department of Homeland Security, 2012), http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf.

[161] "National Network of Fusion Centers Fact Sheet," accessed January 15, 2014, https://www.dhs.gov/national-network-fusion-centers-fact-sheet#1.

criticized and led to an increased emphasis for government organizations to share information.[162]

In 2005, a meeting of the NGA led to the publishing of a 2006 survey of state homeland security advisors and "found that developing a state intelligence fusion center ranked as their third priority." The survey and conclusions followed a 2005 Homeland Security Advisory Council (HSAC) meeting in March 2005 that found, "each state should establish an information center that serves as a 24/7 'all source', multi-disciplinary, information fusion center."[163]

In 2006, Charles Allen, Under Secretary for DHS's Office of Intelligence and Analysis submitted a fusion center plan of action to then DHS Secretary Michael Chertoff. Charlie Allen outlines the fusion centers' potential to aid federal counter-terrorism efforts. In the memorandum, Mr. Allen stated, "We need the capability to routinely harvest information and finished intelligence in a timely manner from State and Local sources." And fusion centers were "one of the most important endeavors the Department can undertake right now."[164] Secretary Chertoff signed off on the plan later that year, and the fusion center concept took on increased level of energy in the number of centers created and the monetary funds allotted to the program.

B. NUMBER OF FUSION CENTERS IN THE NATIONAL NETWORK

> As of September 1, 2007, 58 fusion centers were either operating of being established. By the end of 2011, there were 77 fusion centers within the National Network, and with the January 2013 designation of a fusion center in Guam, there are no 78: 52 State and territorial and 26 Major Urban Area fusion centers. CHS SLFC Report 2013 Final[165]

---

[162] The National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington, DC: National Commission on Terrorist Attacks Upon the United States, 2004), ch. 13, http://govinfo.library.unt.edu/911/report/911Report_Ch13.pdf.

[163] John Rollins, *Fusion Centers: Issues and Options for Congress* (CRS Report No. RL34070) (Washington, DC: Congressional Research Service, 2008), https://www.fas.org/sgp/crs/intel/RL34070.pdf.

[164] United States Senate, *Permanent Subcommittee on Investigations, Federal Support for and Involvement in State and Local Fusion Centers*.

[165] Committee on Homeland Security, *CHS SLFC Report 2013 Final* (Washington, DC: Committee on Homeland Security, 2013), 16, http://homeland.house.gov/sites/homeland.house.gov/files/documents/CHS%20SLFC%20Report%202013%20FINAL.pdf.

In 2008, a CRS report to Congress entitled *Fusion Centers: Issues and Options for Congress*, identified four fusion center value propositions:

- Intelligence, and the intelligence process, plays a vital role in preventing terrorist attacks
- The fusion of a broader range of data, including non-traditional source data, is essential in creating a more comprehensive threat picture.
- State, local, and tribal law enforcement and public sector agencies are in a unique position to make observations and collect information that may be central to the DNI's annual threat assessment.
- Having fusion center activities occur at the sub-federal level can benefit state and local communities, and possibly, has national benefits as well.[166]

In 2009, DHS Secretary Janet Napolitano said during her speech at the Council of Foreign Relations, "Fusion centers are and will be a critical part of our nation's homeland security capabilities. I intend to make them a top priority for this Department to support them, build them, improve them and work with them."[167] With the increase in support for the fusion centers, some have also rebuffed the mission and worth of the centers. Although, six years later, a review of the value propositions previously listed states that a cyber mission uniquely fits into the fusion center operational mission.

C. FUSION CENTERS—A CYBER MISSION

In July 2013, discussions concerning fusion centers relating to the Majority Staff Report on the National Network of Fusion Centers from the Committee on Homeland Security and the October 3, 2012, U.S. Senate Permanent Subcommittee on Investigation, found "that DHS' work with those state and local fusion centers has not produced useful intelligence to support federal counterterrorism efforts."[168] The Senate report is completely contrary to the March 2012 NPR, which key findings stated, "A network of

---

[166] Rollins, *Fusion Centers: Issues and Options for Congress*.

[167] "Remarks by Secretary Napolitano at the Council on Foreign Relations," July 29, 2009, http://www.dhs.gov/ynews/speeches/sp_1248891649195.shtm.

[168] Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, *Federal Support for and Involvement in State and Local Fusion Centers Majority and Minority Staff Report Permanent Subcommittee on Investigations United States Senate* (Washington, DC: United States Senate, 2012), http://cdn.govexec.com/media/gbc/docs/pdfs_edit/100312cc1.pdf.

state and major urban fusion centers and Joint Terrorism Task Force (JTTF) has significantly improved analytical and information sharing capabilities among law enforcement, homeland security, and Intelligence Community entities at all levels of government."[169] The NPR used a survey to obtain its analysis. The Subcommittee on Investigations reviewed reports, visited fusion centers, and analyzed budget decisions, in comparison to DHS requirements. Although the Subcommittee report is very critical of the fusion centers, the recommendation section holds optimism that the problems can be corrected.

The first recommendation by the Senate Subcommittee on Investigations was for DHS to "conform its efforts to match its counterterrorism statutory purpose, or redefine DHS' fusion center mission."[170] From a cyber mission perspective, the fusion center profile has the authority, organizational structure, organizational collaboration framework, personnel, and mission delegation to absorb a cybersecurity mission for the protection of SLTT governments' computer networks. Throughout the country, several fusion centers have the infrastructure and operational processes in place to incorporate a cyber mission. The next section reviews these fusion centers.

1. Fusion Centers—Cybersecurity Today

The Cyber Intrusion Center (City of Los Angeles) launched in 2013 and builds upon the work of 2012 Naval Postgraduate School Center for Homeland Defense and Security graduate John Zambri, Los Angeles, California Police Department Detective in building the foundation and establishing the Cyber Intrusion Command Center (CCIC) operational structure.[171] The center is controlled by the Los Angeles Police Department (LAPD). The 24/7 cyber center has inventoried all the government-owned computer networks and is in the process of patching and hardening its infrastructure. The city also

---

[169] FEMA, *National Preparedness Report* (Washington, DC: FEMA, 2015), 12, http://www.fema.gov/national-preparedness-report.

[170] U.S. Government Accountability Office, *Cybersecurity: Threats Impacting the Nation, Statement of Gregory C. Wilshusen, Director, Information Security Issues* (GAO-12-666T) (Washington, DC: U.S. Government Accountability Office, 2012), http://www.gao.gov/assets/600/590367.pdf.

[171] "CHDS Grad Steers L.A.'s Unique Cyber-Intrusion Center," accessed February 23, 2014, http://www.chds.us/?press/release&id=3086.

monitors all physical police activity throughout the city.[172] The center provides a model for the combined interaction of cyber and physical security.

In January 2013, the state of New Jersey opened its Cyber Fusion Cell within its Regional Operation Intelligence Center. The Cyber Fusion Cell focuses on sharing cyber threat information by working with the public and private sector. The cyber effort is led by the state CIO and has initiated a series of exercises to test its processes and procedures. The state uses its own assets to monitor and harden government computer networks. The Cyber Fusion Cell reports information using a tool called the "Suspicious Activity Reporting System," the same alerting system used by law enforcement that provides for increased collaboration and unity of effort.[173]

In Michigan, during the state's 2013 Cyber Summit, Governor Rick Snyder introduced a volunteer IT force to help the state deal with cyber attacks. The governor's goal was to provide a broader network of cyber responders.[174] In June 2014, Michigan had built the small volunteer corps into a group of trained cyber experts. The program is called the Michigan Cyber Civilian Corps (MIC3). The group correlates cyber information with government, private, education, and business sectors.[175]

In February 2013, The Louisiana State Analytical and Fusion Exchange (LA-SAFE) responded to a sheriff's department request that its telephone lines were intentionally being flooded with 200 telephone calls per minute (DDoS attacks), rendering its 911 service inoperable. LA-SAFE released an advisory through the fusion centers, municipal agencies, critical infrastructure network, and law enforcement. The collaboration revealed over 500 such attacks occurring across the nation. The successful

---

[172] Colin Wood, "L.A.'s Cyber Intrusion Command Center: A Model for Cybersecurity Governance?," Emergency Management, May 27, 2104, http://www.emergencymgmt.com/safety/LAs-Cyber-Intrusion-Command-Center-Cybersecurity.html.

[173] Brian Heaton, "New Jersey's Cyber Fusion Cell Collaborates on Cyberthreats," Emergency Management, September 23, 2013, http://www.emergencymgmt.com/safety/New-Jerseys-Cyber-Fusion-Cell.html.

[174] Hilton Collins, "Michigan Launches Volunteer Cybersecurity Corps," October 25, 2013, Government Technology, http://www.govtech.com/security/Michigan-Launches-Volunteer-Cybersecurity-Corps.html.

[175] "About MiC3," accessed March 11, 2016, http://www.micybercorps.org/about.php.

collaboration led to the establishment of a national task force to identify and find those responsible. LA-SAFE's cyber division was formed in response to the Conficker worm in 2009.[176]

In November 2013, the New York State Intelligence Center relocated to the Center for internet Security (CIS). "CIS is a global non-profit organization whose mission is to enhance cybersecurity readiness and response of the public and private sectors."[177] The relocation of the intelligence center with the cyber organization "creates a joint operations and analytical unit to more effectively analyze and respond to cyber-occurrences."[178] This concept is a model partnership for fusion centers to absorb a cyber mission. The ability to collaborate with a nonprofit organization provides a strategy to leverage existing capabilities to reduce cost, strengthen partnerships, and coordinate SLTT computer network protection.

Two initiatives at the federal-level has also proven that the fusion center model has the capability to absorb a cyber mission. The next section reviews the DHS Fusion Center Pilot concept and the National Guard's cyber security civil support team strategy.

2. Federal Support to the SLTT Cyber Mission

The 2014 DHS Fusion Center Pilot (mature cyber capability) is a concept similar to the main thrust of this thesis. The Pilot is designed to develop a specific fusion center framework to assess the viability of absorbing a cyber mission into the center. The Pilot is currently designed to leverage mature fusion centers in San Francisco, CA, Baton Rouge, LA, Kansas City, MO, Madison WI, and East Greenbush, NY. The concept includes an advisory board that has identified 10 tasks to be implemented in the initiative. The tasks range from information sharing and training to a detailed budget. The Pilot has

[176] Melissa Delaney is a freelance journalist who specializes in business technology She is a frequent contributor to the CDW family of technology magazines. Melissa Delaney, "Fusion Centers Provide Critical Link in Cybersecurity," StateTech, April 7, 2014, http://www.statetechmagazine.com/article/2014/04/fusion-centers-provide-critical-link-cybersecurity.

[177] StateScoop Staff, "New York Cyber Fusion Center to Relocate to CIS," *StateScoop*, accessed March 15, 2016, http://statescoop.com/new-york-cyber-fusion-center-relocate-cis.

[178] Ibid.

been signed by representatives from the Office of the Director of National Intelligence (ODNI), DHS, NFCA (National Fusion Center Association), IACP (International Association of Chiefs of Police), and CIS. The success of the pilot will be released in an upcoming report.

3. Cyber Security Civil Support Teams (National Guard)

As discussed in the previous chapter, the Cyber Warrior Act of 2013 would set up Cyber and Computer Network Incident Response Teams (CCNIRTs) in each of the 50 states and four U.S. territories. CCNIRTs, once activated by the governor or secretary of defense, will respond to a cyber attacks.[179] As discussed, the states believe Guard mobilization against cyber attacks can play a critical role in the defense of state and local networks. The ability to leverage the experience of IT professionals at a fairly low-cost is a very attractive option in the fight against malicious cyber actors and criminals. The key advantage to this concept is the governor is involved in the decision-making process. For the cyber teams to be activated, the governor must have knowledge of the details of the cyber event. The disadvantage, the cyber attack has already happened; the activity is by nature reactive, and no prevention stage occurs. The key is to understand the TTPs of the cyber actor and use the TTPs to prevent future threats.

4. Challenges to the Fusion Center Cyber Mission

A report by the Ponemon Institute in October 2015 identified 86% of respondents in state and local government believe the responsibility for managing cybersecurity risk in their organizations is the most stressful job they have.[180] This stress is impacted by many characteristics but this study reviews three key attributes: budget, personnel, and organizational plans.

---

[179] Mickey McCarter, "U.S. National Guard: Senators Seek National Guard Cybersecurity Civil Support Teams," Homeland Security Today, March 27, 2013, http://www.hstoday.us/channels/us-national-guard/single-article-page/senators-seek-national-guard-cybersecurity-civil-support-teams/8461dd77befa9b1506273a976c5c2b15.html.

[180] "The State of Cybersecurity in Local, State and Federal Government," October 9, 2015, http://www.ponemon.org/blog/the-state-of-cybersecurity-in-local-state-and-federal-government.

a. Budget

The typical SLTT entity "spends less than 5% of its IT budget on cybersecurity."[181] Although, the state of Michigan increased its budget by $5 million in 2016, a 2.4% increase in cybersecurity.[182] Every state places a different priority on cyber. This priority normally is directly related to their budget. States need to focus on cybersecurity through their budget and cybersecurity professionals to protect their networks and sensitive information.

b. Personnel

With the continuous increase in internet usage, experienced cyber security personnel are needed. This need is at the federal and state level. However, a look at the state challenge was identified in a 2015 report by the National Association of State Chief Information Officers, which surveyed 49 state CIOs concerning the challenge to hire and retain cybersecurity personnel. The following statistics are provided:

- Nearly 92% of states say salary rates and pay grade structures present a challenge in attracting and retaining IT talent.
- 86% of states are having difficulty recruiting new employees to vacant IT positions.
- 46% of states report that it is taking 3–5 months to hire senior level IT positions.
- A shortage of qualified candidates for state IT positions is hindering 66% of states from achieving strategic IT initiatives.
- Security is the skill that presents the greatest challenge in attracting new employees.[183]

---

[181] Paul Lipman, "4 Critical Challenges to State and Local Government Cybersecurity Efforts (Industry Perspective)," Government Technology, July 17, 2015, http://www.govtech.com/opinion/4-Critical-Challenges-to-State-and-Local-Government-Cybersecurity-Efforts.html.

[182] Gongwer, "New State Budget Would Give $5 Million Boost to State Cybersecurity Protection," February 11, 2016, Mitechnews.Com, http://mitechnews.com/politics/new-state-budget-would-give-5-million-boost-to-state-cybersecurity-protection/.

[183] "State IT Workforce: Facing Reality with Innovation," April 2015, http://www.nascio.org/Publications/ArtMID/485/ArticleID/79/State-IT-Workforce-Facing-Reality-with-Innovation.

c. Plans

A 2015 study by the Pell Center entitled, *State of the States on Cybersecurity*, identified where the state stands in its maturity and commitment to cybersecurity based on five operational areas: state cybersecurity strategic plans, incident response, E-crime and law enforcement, information sharing, and cyber R&D, education, and capacity building.[184] If states had established any progress in these areas, they were given at least partial credit during the assessment. A total of eight states (CA, MD, MI, NJ, NY, TX, VA, and WA) were selected to participate in the assessment based upon the states' priority on cybersecurity. The results of the assessment identified gaps within each state, but mostly within the strategic plan area. Each state had gaps in most of the evaluation areas, with Michigan appearing the most prepared amongst all eight states. This study would be effective for every SLTT entity, as the assessment methodology allows the state to perform an evaluation of its cybersecurity operational space. The assessment provides practical ways for state and local governments to take inventory of their cyber assets, strategies, and policies.

This chapter looked at the fusion centers' mission and provided examples of several fusion centers throughout the United States that have absorbed a cyber mission. The analysis provided an examination of why fusion centers were created and the realization of utilizing fusion centers in the fight to protect SLTT computer networks. The fusion center mission is designed to defend the nation and the states against emerging threats. In addition, the cybersecurity arena is no longer just an emerging threat. U.S. computer networks are being attacked from all angles. SLTT computer networks will undoubtedly become an increasing target of opportunity for the cyber criminals, hackers, extremists, or nation-state actors. As stated earlier, the NASCIO study reported that only 24% of state officials say they are very confident in protecting their states' computer assets against external threats.[185] With only 24%, how can the confidence level of state CIO's be increased? The next chapter discusses protecting SLTT computer

[184] Francesca Spidalieri, *State of the States on Cybersecurity* (Newport, RI: Pell Center, 2015), http://pellcenter.org/wp-content/uploads/2015/11/Pell-Center-State-of-the-States-Report.pdf.

[185] National Association of State Chief Information Officers (NASCIO), *2012 Deloitte-NASCIO Cybersecurity Study, State Governments at Risk: A Call for Collaboration and Compliance*, 3.

networks by utilizing fusion centers to incorporate a cyber mission by infusing cyber security teams into fusion centers specifically to perform this function. Why specific cyber security teams? The answer goes back to 2006 when the U.S. Department of Justice developed the fusion center guidelines. The process of securing SLTT computer networks will be enhanced if all fusion centers establish a cyber mission designed to protect the states' computer networks and share computer-related threat information across the country. All fusion centers should incorporate a baseline cyber framework that includes infrastructure, personnel, reporting capability, incident response capability, intrusion detection capability, and information sharing with state, local, and federal partners. Chapter VII explores the incorporation of an adjunct cyber mission for fusion centers across the United States in an effort to protect SLTT computer networks.

VII. FUSION CENTERS: A CYBER INITIATIVE

As discussed throughout this thesis, the cyber threat today is constantly evolving and has a direct impact on America's national security. Cyber criminals are continually looking for new and inventive ways to access government files, steal intellectual property, access banking system data, steal PPI through retail outlets (e.g., Target and Lowe's), health care sponsors (Anthem), industry organizations (Sony), government organizations (OPM) and educational institutes (University of Maryland) to name a few. A review of the literature details various strategies, collaboration efforts, and plans to assist SLTT entities in their defense of cyber networks. The problem is no standard cyber blueprint or unity of effort exists amongst the fusion centers to incorporate a cyber mission. Several ideas have been pulled together depending upon state or local needs and current operational capability. What is lacking is a consolidated strategy and framework on how to best incorporate the cyber threat faced by SLTT entities. This chapter proposes a strategy to overcome this challenge.

A. CRYPTOLOGIC SUPPORT TEAMS

In 2007, during the second Iraq War, at the onset of the "surge" of U.S. military ground forces, the United States also made a change to its intelligence collection efforts. This collection focus allowed the United States to gain the tactical advantage in the war. A change in leadership at the combat support agencies led to a change in strategy to implement new technology and innovation tools that enhanced the TTPs from lessons learned on the battlefield. The United States initiated an *intelligence-driven operations model* that was highly effective.[186] Can this cryptologic support group concept be incorporated in fusion centers to leverage the federal government capabilities and tackle the cyber challenge?

[186] Barry Harris, "Stabilizing Iraq: Intelligence Lessons for Afghanistan," The Washington Institute, May 29, 2009, http://www.washingtoninstitute.org/policy-analysis/view/stabilizing-iraq-intelligence-lessons-for-afghanistan.

The CSG concept was designed by the U.S. intelligence community to provide dedicated intelligence support to military commanders or other U.S. government departments or agencies during a time of war or crisis.

The CSG organizational construct can either be distinct and centrally located within the customer space to provide broad support to a customer across a range of cryptologic issues, or a combination of centrally located entities along with individuals integrated into a specific regional and functional area to provide subject matter expertise within the customer environment.

Customer relations functions include facilitate the intelligence process, provide intelligence expertise to a customer or region, educate the customer, provide direct reach back to home base, and provide direct 24x7 watch operations support. Can this cryptologic support groups concept can possibly be utilized to help protect cybersecurity networks of SLTT governments?

B. CYBERSECURITY SUPPORT TEAMS

This thesis proposes a concentrated effort to integrate cyber teams into fusion centers. This concept requires a baseline cyber team to be established with a fusion center. The teams will be built using current federal staffing with additional staffing hired by the state and local government. Training will be required to ensure cyber teams are trained to a specific standard and incorporated directly into the fusion center with the authority and ability to provide direct support through dynamic cyber defense capabilities with tools and cyber intelligence leveraged from federal government cyber centers. The ability to leverage federal cyber center assets to provide a focused dynamic defense capability directly to SLTT assets through the fusion center is an option discussed in the previous chapter and is being utilized today.

The initial core capability would focus on the following five mission areas: state government, education, health care, banking and finance, and critical infrastructure networks. The protection of PII would be given maximum security consideration within the five mission areas.

The improved intelligence capabilities allowed the coalition forces to be proactive rather than reactive. An adjustment in TTPs allowed for the disruption of activities during the planning or implementation phase of the adversaries operations. When knowing and understanding the adversary's TTPs, it is easier to disrupt prior to an incident or set up traps and lay in anticipation of the adversaries moves.[187]

The use of signals intelligence (SIGINT) during the first Gulf War is a key aspect of the intelligence driven operations model that is a viable option in the fight against cyber terrorism. NSA pushed cryptologic support teams down to the battalion level to provide direct support to the theater and the commanders on the battlefield. The advantage was that intelligence was more timely and relevant. Moreover, because NSA was controlling the intelligence process, it was able to synergize operations effectively. Another key advantage was the feedback loop, with weekly meetings and video teleconferences, collection and mitigation that allowed for an active sharing of critical information. This concept of deploying cryptologic support teams forward also played a big role (with the same success rate) in Afghanistan. One of the challenges of forward deployed teams in Afghanistan was the sharing of intelligence without divulging sensitive collection methods.[188]

The concept of forward deployed cryptologic support teams can be utilized within the cyber domain to provide cyber support to SLTT governments. The success of an intelligence driven operational model that controls and synergizes dynamic cyber defensive engagement, targeted at specific TTPs, can be utilized in fusion centers around the country to deter the threat and protect sensitive networks.

C. A NEW APPROACH

As detailed in Chapter II, nation-state actors, terrorists, criminals, and hacktivists are targeting U.S. computer networks at a constant and increasing rate. State and local government officials have only a 24% confidence level that they can protect their

[187] Ibid.

[188] Ibid.

computer networks from attack. The cyber threat to the U.S. is growing and described in Figure 1.

(1) Policy Development and Legal Framework

This agreement or understanding is critical for operational success. The Cybersecurity Defensive Engagement Support Teams (CDEST) should have the authority to provide direct support to SLTT stakeholders. The primary success of the concept is to allow the teams direct access to state government networks. The only way to achieve this goal is under direct authority of the governor. The teams will be operationally organized, using existing manpower from federal, law enforcement, state and local, and if needed, National Guard personnel. The governor or the state chief information actor (acting on behalf of the governor) will provide oversight and direct cybersecurity support to the state's computer networks. The teams will function under the same authorities as the current personnel.

(2) Federal and State Relationships

A MOA should be established between the state governor and the Secretary of Homeland Security. This agreement is similar in purpose, scope, mission, and responsibilities as signed in 2010 between DHS and DOD. The agreement encourages interdepartmental collaboration, "mutual support for cybersecurity development, and synchronization of current operational cybersecurity mission activities."[189] The governor has the power to control state-owned assets. The CDEST is designed to provide hands-on cyber support to state-owned assets (state government, educational institutions, banking and financial institutions) (regulated by state government), health care exchanges, and critical infrastructure assets. If a state-owned or operated institution (e.g., University of Maryland) is involved in a cyber-attack, the CDEST will have the authority to go to the University of Maryland and take the lead role in determining the identification, detection, mitigation, and recovery of the computer network. Through collaboration efforts, the

[189] Department of Homeland Security, *Memorandum of Agreement between the Department of Homeland Security and The Department of Defense Regarding Cybersecurity* (Washington, DC: Department of Homeland Security, 2010), http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf.

CDEST will provide training, collaboration, system testing, and network resilience efforts to strengthen and fortify networks.

(3) Infrastructure Assessment

The 74 fusion centers spread across the nation are all at different levels of operational maturity, cyber maturity, personnel maturity, and mission capability. These levels of maturity and capability will be addressed as the CDEST teams are deployed to the fusion centers. However, prior to deployment, a certain level of physical and information infrastructure is required to be in place.

(4) Physical Infrastructure (Facility Assets, Communication Security)

The facility should be equipped to handle all three levels of information (unclassified, secret, and top secret). The facility would conform to DoDM 5105.21-Vol 1–3, Sensitive Compartmented Information (SCI) Administrative Manual and Intelligence Community Standard Number 705–1 (ICS 705–1) Physical and Technical Security Standard for Sensitive Compartmented Information Facilities (SCIF) (Effective: 17 September 2010). The facility should be accredited and TEMPEST tested. A benefit concerning the physical infrastructure requirements are many fusion centers have been built to SCIF standards.[190] The positive aspects of the facilities' physical infrastructure also provide for greater access to information data sources without incurring additional cost.

(5) Identify Data Sources

All fusion centers should have access to a general suite of communication data sources. Access to unclassified information through the MS-ISAC (cyber threat reporting) and NCCIC (cyber information sharing portal G-FIRST) is required. Access to secret information through the DHS' Homeland Secure Data Network (HSDN) network and FBI's Guardian Automated Case Support (ACS) network is required. Access to top

[190] Stephen Serrao, "Fusion Centers: Defining Success," Homeland Security Today, October 13, 2009, http://www.hstoday.us/blogs/best-practices/blog/fusion-centers-defining-success/d2adf8a8025faecbe0268d81fe1d3c54.html.

secret information is required through the Joint Worldwide Intelligence Communications System (JWICS) network and FBI's SCI Operational Network (SCION) network is required. These information sources provide a basic level of communication data sources that will allow for efficient operational information sharing activities.

(6) Enhance the Reporting Network

The information data sources noted previously allow for the construction of efficient information-sharing processes with the six federal cyber centers through the MS-ISAC. As discussed in Chapter III, the MS-ISAC was established to provide cyber information sharing and cybersecurity defense directly to SLTT entities.

The federal cyber centers can communicate directly with the fusion centers for time-sensitive information or through the MS-ISAC during normal reporting and analysis procedures. This process is very similar to the Interagency Sharing Environment (ISE) Interagency Threat Assessment and Coordination Group (ITACG) framework. The mission will dictate reporting requirements and be flexible enough to surge communication avenues when needed.

(7) Build Cybersecurity Teams

The CDEST team should include the main key skill sets, as described in the Cyber Security and Information Assurance Green Hat Philosophy. The skill set includes incident response, critical infrastructure protection, containment, eradication, and recovery, malware analysis, resilience and business continuity. These skill sets are universal (with some variations) throughout the cyber security and information assurance industry. The structure and skill set of the team will incorporate known cybersecurity experience. The need for a well-rounded team is essential for operational success. The team of experts should have the ability to work hand-in-hand with SLTT stakeholders. The team will have the authority of the governor and Secretary of Homeland Security. Figure 3 is a breakdown of the team and the operational responsibility for each member.

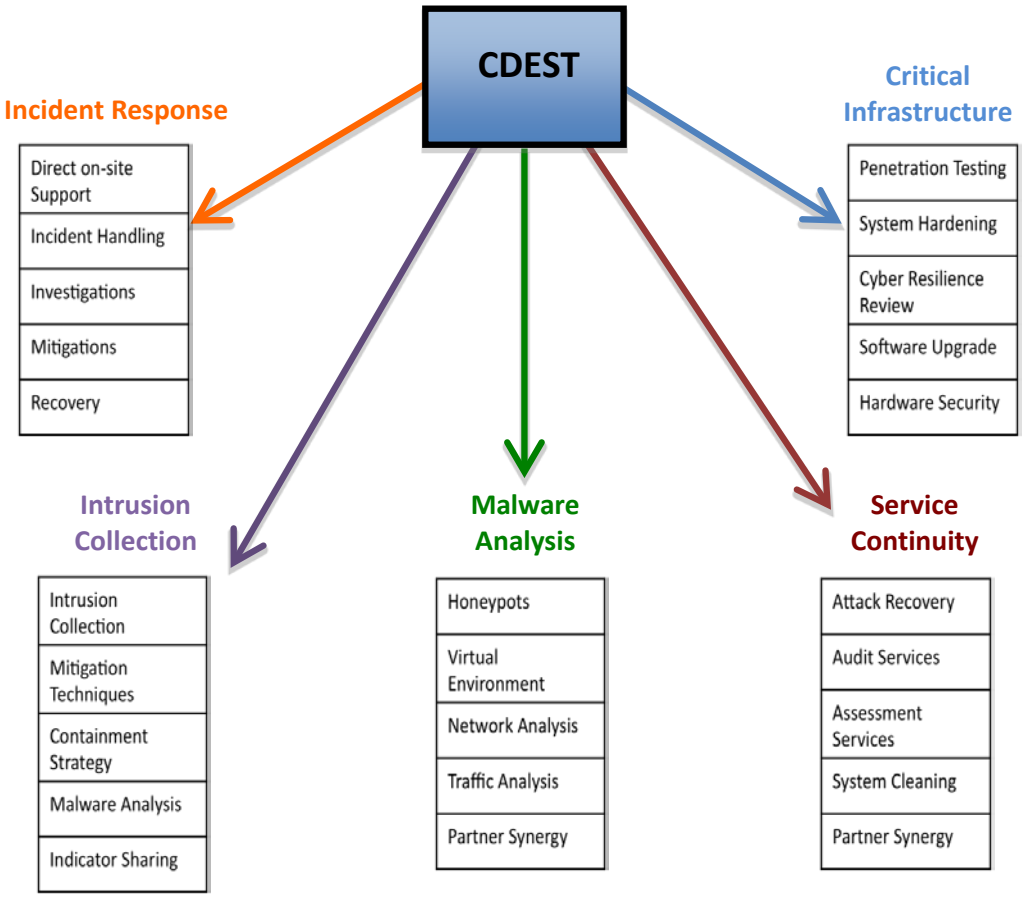

Figure 3. Fusion Center Cyber Responsibilities[191]

(8) Identify Cybersecurity Training

The training effort will be designed to familiarize the team with the federal cyber security centers, SLTT stakeholders, ISACs, and the organizations within the ISEs. Specific training will incorporate access and utilization of the data sources referenced above. The need to leverage the data sources for the good of the SLTT stakeholders is one of the primary goals of the team.

D. IMPACT TO THE SLTT GOVERNMENTS

The goal of this strategy is to integrate CDEST s directly into state and major urban area fusion centers. The CDEST teams will provide direct cybersecurity support to

[191] Adapted from "Information Assurance Philosophy—Green Hat, Cyber Security and Information Assurance," https://www.mile2.com/ia-philosophy.html?tmpl=component&print=1&page=.

SLTT governments. The teams will have the authority to interact with cybersecurity defense, mitigation, recovery, and prevention. The primary advantage would be the synthesis of the state and local government stakeholders to provide a robust dynamic cyber defense capability from the bottom-up.

E. VALUE PROPOSITION AND RISK

The introduction of a dedicated cybersecurity mission into the fusion centers will allow for a dynamic cyber defense capability, interactive information-sharing process between the federal government and SLTT governments, and a whole-of-government approach to protecting the nation's cyber networks. This cybersecurity framework and strategy will provide value at both the state and federal level of government, as shown in Figure 4.

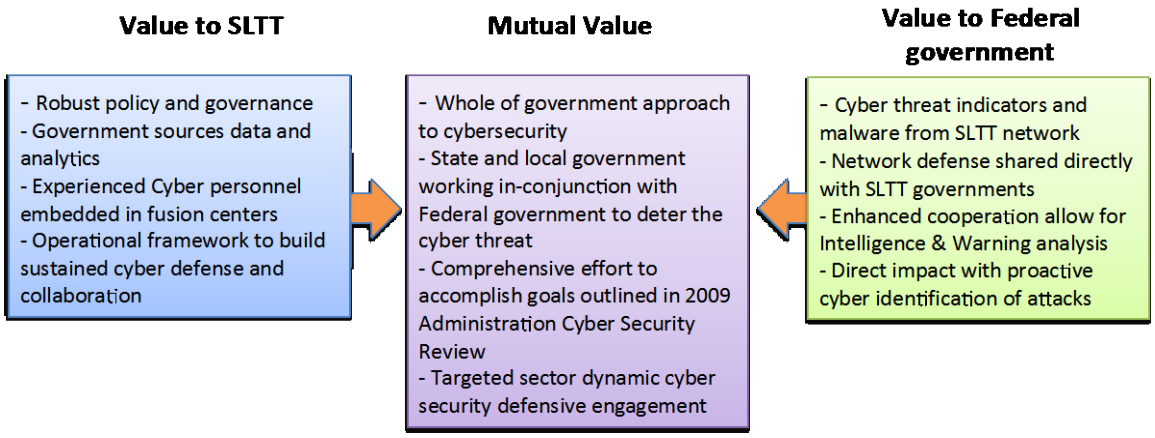

Figure 4. Cyber Fusion Center Value Proposition

(1) Value to SLTT Government

SLTT entities will benefit greatly from dedicated cyber personnel imbedded directly into the fusion centers. The personnel will benefit from a robust policy and governance between the governor and the Secretary of Homeland Security. The authority from the governor allows the cyber security teams to work directly (and if needed onsite) with the stakeholders' cybersecurity teams. This face-to-face interaction is a 360-degree

change from the current process in which many fusion centers currently have no cyber personnel onsite. The fusion centers with no cyber personnel are basically transit centers used to push the information to organizations or personnel of interest. In this new framework, cyber information will be processed and analyzed for actionable information, the data can be provided directly to stakeholders, and the cyber personnel can work directly onsite to ensure the proper application of the information or identification of threats to the computer network. The framework has the potential to build a sustained cyber defense and collaboration effort that is greatly needed to protect SLTT government networks.

(2) Value to the Federal Government

A framework that allows actionable cybersecurity information to be shared and acted upon with SLTT governments is a win-win for federal government partners. Many times, information is shared with SLTT government entities, but because of information security barriers, the classification level of the information, and the ability to share information with cybersecurity personnel in a position to act on the data, the information-sharing process breaks down. A framework to share actionable data, at all three classification levels to cybersecurity teams with the ability to act as a standalone defense mechanism, or in-conjunction with the cyber teams affected by the unwanted network intrusion, or the ability to share defensive strategies to prevent the threat, is critical to the protection of computer networks at all levels of government. This enhanced level of cooperation allows for indications and warning prior to an intrusion and helps the federal government be proactive in its cyber defense engagement rather than reactive.

(3) Mutual Value

The mutual value of the imbedded cyber security teams in fusion centers is the ability to enact a whole-of-government approach to protecting the country's cyber security networks. In May 2009, President Obama said "cybersecurity is one of the most serious economic and national security challenges we face as a nation"[192] One of the

[192] "The Comprehensive National Cybersecurity Initiative."

goals of the Comprehensive National Cybersecurity Initiative (CNCI) was to "establish a front line against threats by creating shared situational awareness of network vulnerabilities, and threats."[193] This framework allows for the CNCI goal to be realized. The framework that provides a front-line defense for SLTT governments will also be of great benefit to the federal cyber centers through the sharing of indicators and actionable cyber intelligence that can be used to identify the TTPs of the adversary. The TTPs can be used to build a better security mechanism to protect computer networks against future cyber attacks and unwarranted intrusions. This mutual benefit will be shared by both federal and SLTT governments as summarized in Figure 5.

(4) Risk

The risk of inaction places SLTT governments in a continuous cycle of proactive response to cyber attacks and intrusions. A fusion center cyber team with the authority of the state governor to support and defend the computer networks of state government assets provides an idea solution against the current threat environment.

[193] Ibid.

F. IMPLEMENTATION: TIMEFRAME AND COST

The implementation of this process is accomplished in four phases, as seen in Figure 5. The phases are interdependent. One process does not need to be completed before the other processes start.

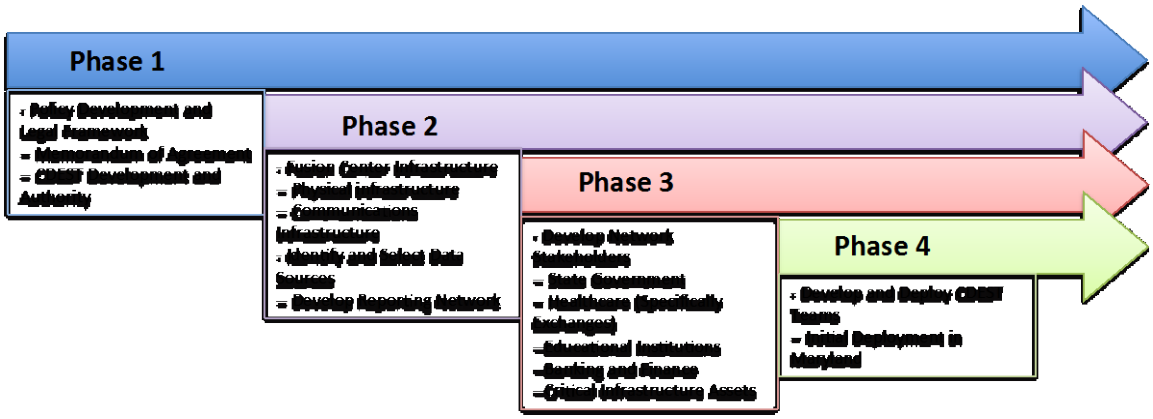

Figure 5. Cyber Fusion Center Implementation Plan

(1) Phase I: Framework

The governor as the leader and owner of state assets must support the framework. The Secretary of Homeland Security as the federal agent with ultimate responsibility for the care, feeding, and direction of the fusion centers must support the framework. The MOA that provides the authority for the development and operational framework of the CDEST teams is the key to the success of the strategy.

(2) Phase II: Infrastructure

Identification, assessment, development, accreditation, and certification of the fusion center physical infrastructure are undertaken in the second phase of the framework. The communications infrastructure is also put in place during Phase II. This phase ensures the interoperability amongst federal agencies and SLTT governments. A standard and repeatable physical infrastructure is identified and incorporated with a specific set of standardized data sources. The key is to develop a secure and standardize infrastructure that can be replicated throughout the country.

(3) Phase III: Implementation

Phase III corresponds with Section Five of the implementation plan. Initially, the cyber teams deployed to the fusion centers would engage five sectors within the state's infrastructure: state government, educational institutions, banking and finance, healthcare, and critical infrastructure. These five sectors may be expanded as the maturity of the teams and the processes mature. However, the cyber domain and threat is so large and evolving so quickly that it is important that the teams do not try to be all things to all people and organizations. The initial process will build network maps, identify network security processes, identify and communicate directly with security operations center personnel at the stakeholder's organization, identify strengths and weaknesses in the stakeholder's computer network, and incorporate security upgrades as needed.

(4) Phase IV: Cybersecurity Teams

In this final phase, the CDEST teams will be developed as an integrated group of cyber professionals at the GS-11 through GS-14 level. This level provides a mix of experience that will allow for current and future requirements. The primary lead for the team can be a GS-15. The DHS CSA concept discussed earlier will normally be designated as the lead for the team. The team will consist of an FBI representative, a state representative, a National Guard representative, and the fifth billet can be filled by any of the four organizations. The key for the team is to be organized jointly from a homeland security, law enforcement, state, and National Guard representative perspective. The second important aspect is the qualifications. The team must have mid-level to senior-level personnel with computer experience. The team will work at the cross-section between federal and state organizations. They will have the authority to access stakeholder's computer networks and they will have a tool set to allow them to provide state-of-the-art cyber security support. All four phases of the framework can be accomplished within a six-month timeframe, at minimal cost, and the teams can be in the cyber center and operational.

So far, the study has focused on federal assets but the state and local governments must take a lead role in developing the cyber workforce of the future. "Hiring new

employees, training or retraining current employees and contracting out for cybersecurity services are three ways that states can meet their needs."[194] Another key resource is the state colleges and universities. The state and local governments would be wise to start a partnership with state higher education institutes to establish a pipeline to hire young graduates (lower initial payroll cost although it may also be a higher turnover rate after two years) and provide an opportunity to work immediately after graduation.

Another source of a cybersecurity workforce are the states' National Guard units. During last year's NGA Forum on Cybersecurity, Lieutenant General Ed Cardin of the USCC "highlighted the Kansas Intelligence Fusion Centers' intelligence program as a nation-wide model and best practice with private sector partners."[195] He also commented on the success of the small teams utilized during the Iraq War for intelligence purposes as discussed previously. The key is to utilize multiple sources to staff the fusion centers.

(5) Costs

The framework will use existing infrastructure (physical and communications) and existing personnel currently in the system. Both DHS and DOJ have personnel who can be reassigned to the fusion centers in support of cyber operations. Since the cyber expertise is not currently in place, the manning structure will need to be adjusted and the familiarization training will be required to ensure the cyber team has a clear understanding of the capabilities and mission functionality available to them at the federal level. Also, familiarization will be needed to understand the structure of the SLTT government stakeholder networks.

G. MEASURING SUCCESS

Success is measured through the ability of the cybersecurity teams to process actionable information and interact with stakeholders within the five targeted sectors and provide dynamic cybersecurity defensive protection measures, as well as by the

[194] National Governors Association, Cybersecurity Workforce Key To Combating Threats, October 27, 2014, http://www.nga.org/cms/home/news-room/news-releases/2014--news-releases/col2-content/cybersecurity-workforce-key-to-c.html

[195] Sean Lyngaas, "Cyber Threat Challenges Military Structure," The Business of Federal Technology, February 23, 2015, https://fcw.com/articles/2015/02/23/cyber-threat-challenges-military.aspx.

hardening of the computer network infrastructure of SLTT governments. Success is measured through the value proposition as described in the overall whole-of-government strategy. Success can be measured by first using a test case and state to implement the plan. The State of Maryland is located in an optimal location to test this strategy and framework. The six cyber centers are all located within the Washington, DC metro area. The Maryland Fusion Center (MCAC) has the physical and communication infrastructure already in place. The offices of Governor O'Malley of Maryland and Secretary Johnson of DHS are a 45-minute drive away. The State of Maryland computer networks provide fertile ground for the cybersecurity teams forward-deployed to the fusion centers. All four phases of the process can be completed within a six-month timeframe and the teams can be on the ground and operational. The teams have an ample opportunity to test their abilities to deploy tools and techniques shared by federal partners and to interact with state-level stakeholders and asset owners. Similar to the cryptologic support groups described at the beginning of the chapter, the cyber security teams will also be expected to facilitate the cyber intelligence process, provide cyber and computer expertise to the designated five sectors, educate the customer, provide direct reach back to home base and to federal government partners, and provide dynamic cybersecurity watch operations support.

H. CONCLUSIONS AND RECOMMENDATIONS

The research question, Should regional state and local fusion centers assist to prevent, mitigate, and deter cyber threats targeted at state, local, tribal, and territorial (SLTT) entities, was examined during this thesis. The research investigated the organizational and individual damage cyber threats can impose upon state and local government (government, finance, education, and critical infrastructure) computer networks. The research also examined the concept of deploying dedicated cyber support teams directly into local and regional fusion centers to spearhead and standardize a cybersecurity mission to prevent, mitigate, and deter cyber threats targeted at SLTT government computer networks.

The research began by analyzing the cyber threat to the nation. FBI Director Robert Mueller stated, "Terrorism does remain the FBI's top priority, but in the not too-distant-future we anticipate that the cyber threat will pose the greatest threat to our country."[196] The major types of computer system vulnerabilities were examined. In addition, the major cyber criminals and hacktivists who attempt to take advantage of these vulnerabilities for personal gain, to support a specific cause, and in support of a specific entity, were analyzed to understand better the actors behind the computer screens.

The focus of this thesis was to analyze the cyber threat to SLTT entities. The research primarily focused on state government departments and agencies, banking and finance, infrastructure systems, colleges and universities, and PII. How to best protect these SLTT computer networks would be the result of the research.

The research continued with an examination of the fusion centers' mission and the ability of fusion centers to accept a new mission focused on cybersecurity defense, mitigation, and analysis, including the establishment of cybersecurity teams or groups resident within the centers. A strategy for state and regional fusion centers to partner with the federal government's department and agencies in a consolidated cybersecurity mission was provided. Also, as stated previously, a coordinated effort across the fusion center landscape must be made to ensure a cyber security standard or guideline to assist with interoperability and communication across the national network of fusion centers.

The research revealed that fusion centers do have the authority to perform a cyber mission. This authority was granted with the passing of the Homeland Security Act of 2002. Although, the cyber threat was not considered as the fusion center mission was being developed. The threat from cyber attacks was not as prevalent then as it is today. A chart was provided that showed the growth of the cyber threat and examples were provided of fusion centers capable of absorbing a cyber mission. The fusion center is uniquely positioned to absorb a cyber mission and every effort should be made to

[196] Ibid.

establish a standard across the U.S. fusion center network to enhance the cyber protection of SLTT computer networks.

In closing, on April 1, 2015, President Barack Obama said at the signing of an EO, "Blocking the property of certain persons engaging in significant malicious cyber-ended activities. The increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. I hereby declare a national emergency to deal with this threat."[197]

Fusion centers were established with the "ultimate goal to provide a mechanism through which government (federal and state), law enforcement, public safety, and the private sector can come together with a common purpose and improve the ability to safeguard our homeland and prevent criminal activity."[198] By combining President Obama's previous comment with the ultimate goal of the fusion centers, the research question should not be, should regional state and local fusion centers assist to prevent, mitigate, and deter cyber threats targeted at SLTT entities; but, why does not every regional state and local fusion center have a cyber mission with dedicated cybersecurity teams to assist in the prevention, mitigation, and deterrence of cyber threats targeted at SLTT entities? This thesis provides a framework to accomplish the mission to secure SLTT computer networks by incorporating cyber security teams within fusion centers.

[197] "Executive Order—Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities," accessed April 15, 2015, https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

[198] Office of Justice Programs, Bureau of Justice Assistance, *Fusion Center Guidelines Developing and Sharing Information and Intelligence in a New Era* (Washington, DC: Department of Justice, 2006), https://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf.

LIST OF REFERENCES

ABC News. “Intel Heads Now Fear Cyber Attack More Than Terror.” March 13, 2013. http://abcnews.go.com/Blotter/intel-heads-now-fear-cyber-attack-terror/story?id=18719593.

Bain, Ben. “DHS, Industry to Try Fusion Centers for Classified Data Swap.” Federal Computer Week, March 16, 2010. https://fcw.com/articles/2010/03/16/web-cyber-threat-fusion-center.aspx.

Burlington Free Press. “State Confirms Health website Security Breach.” Accessed January 21, 2014. http://www.burlingtonfreepress.com/article/20131122/NEWS03/311220030/State-confirms-health-website-security-breach

Campbell, Colin. “More than 309,000 Identities Exposed in University of Maryland Cyberattack.” *Baltimoresun.com*. Accessed March 2, 2014. http://www.baltimoresun.com/news/maryland/bs-md-university-of-maryland-data-breach-20140219,0,2321285.story.

CBSNews. “FBI Investigating Cyber-Attack on Sony Pictures.” Accessed February 18, 2016. http://www.cbsnews.com/videos/fbi-investigating-cyber-attack-on-sony-pictures/.

Center for Digital Government. *Advanced Cyber Threats in State and Local Government*. Folsom, CA: Center for Digital Government, 2014. http://nascio.org/events/sponsors/vrc/Advanced%20Cyber%20Threats%20in%20State%20and%20Local%20Government.pdf.

Center for Homeland Defense & Security. “CHDS Grad Steers L.A.’s Unique Cyber-Intrusion Center.” Accessed February 23, 2014. http://www.chds.us/?press/release&id=3086.

Center for Internet Security. “IP2014 SLTT Government Outlook.” Accessed March 6, 2015. http://iic.cisecurity.org/resources/documents/IP2014SLTTGovernmentOutlook.pdf.

———. “Multi-State Information Sharing and Analysis Center.” Accessed February 13, 2014. http://msisac.cisecurity.org/.

Child, Ben. “North Korea Says Sony Cyber-Attack May Be ‘Righteous’ Work of Its Supporters.” *The Guardian*, December 8, 2014, sec. Film. http://www.theguardian.com/film/2014/dec/08/north-korea-sony-cyber-attack-the-interview.

Cloherty, Jack, and Pierre Thomas. "'Trojan Horse' Bug Lurking in Vital U.S. Computers." *ABC News*, November 7, 2014. http://abcnews.go.com/US/trojan-horse-bug-lurking-vital-us-computers-2011/story?id=26737476.

Collins, Hilton. "Michigan Launches Volunteer Cybersecurity Corps." October 25, 2013, Government Technology. http://www.govtech.com/security/Michigan-Launches-Volunteer-Cybersecurity-Corps.html.

Committee on Homeland Security. *CHS SLFC Report 2013 Final*. Washington, DC: Committee on Homeland Security, 2013. http://homeland.house.gov/sites/homeland.house.gov/files/documents/CHS%20SLFC%20Report%202013%20FINAL.pdf.

ComputerWeekly. "Hacktivism: Good or Evil?." Accessed February 18, 2016. http://www.computerweekly.com/opinion/Hacktivism-Good-or-Evil.

Congress. "Senate Report 114–32, United States Senate S.754—Cybersecurity Information Sharing Act of 2015." Accessed December 28, 2015. https://www.congress.gov/bill/114th-congress/senate-bill/754.

Cowley, Stacy. "FBI Director: Cybercrime Will Eclipse Terrorism." *CNNMoney*, March 2, 2012. http://money.cnn.com/2012/03/02/technology/fbi_cybersecurity/index.htm. This thesis utilizes the analysis method to examine a whole-of-government approach to analyze a strategy or policy that protect SLTT entities better from cyber threats.

Criminal Justice Degree, College, and Career Blog. "Terrorism: Role of Technology in Contemporary Terrorism." Accessed February 19, 2016. http://criminaljusticeonlineblog.com/12/terrorism-role-of-technology-in-contemporary-terrorism/.

CSO Online. "Adobe Confirms Patch for Newest Zero-Day Vulnerability." February 2, 2015. http://www.csoonline.com/article/2878778/application-security/adobe-confirms-patch-for-newest-zero-day-vulnerability.html.

Cyberwarzone. "Anonymous Hackers, Your Unmasked Face Picture Might Be in This List!." Accessed February 12, 2015. http://cyberwarzone.com/anonymous-hackers-unmasked-face-picture-might-list/.

Delaney, Melissa. "Fusion Centers Provide Critical Link in Cybersecurity." StateTech, April 7, 2014. http://www.statetechmagazine.com/article/2014/04/fusion-centers-provide-critical-link-cybersecurity.

Deloitte-NASCIOC. "9326942 NASCIO Cybersecurity Survey." Accessed March 6, 2015. http://www.nascio.org/publications/documents/Deloitte-NASCIOCybersecurityStudy_2014.pdf.

Department of Homeland Security. “About the National Cybersecurity & Communications Integration Center.” Accessed October 16, 2014. http://www.dhs.gov/about-national-cybersecurity-communications-integration-center.

———. “Critical Infrastructure Partnership Advisory Council.” Accessed February 5, 2014. http://www.dhs.gov/critical-infrastructure-partnership-advisory-council.

———. *Critical Infrastructure Protection Advisory Council (CIPAC) Charter* (Washington, DC: Department of Homeland Security, 2010). http://www.dhs.gov/xlibrary/assets/cipac/cipac_charter.pdf.

———. “Cybersecurity and Communications (CS&C).” Accessed February 13, 2014. https://www.dhs.gov/xlibrary/assets/pso_cat_csc.pdf.

———. “DHS State Government Offerings, Products, and Services.” Accessed February 9, 2014. http://www.dhs.gov/sites/default/files/publications/DHS%20State%20Resources_0.pdf.

———. *Enhanced Cybersecurity Services*. Washington, DC: Department of Homeland Security, 2016. https://www.dhs.gov/sites/default/files/publications/ECS-Fact-Sheet_no%20stats_02.2016.pdf.

———. *Fact Sheet: EO 13636 Improving Critical Infrastructure Cybersecurity and PPD 21 Critical Infrastructure Security and Resilience*. Washington, DC: Department of Homeland Security, 2013. http://www.dhs.gov/publication/fact-sheet-eo-13636-improving-critical-infrastructure-cybersecurity-and-ppd-21-critical.

———. “Information Sharing and Analysis Organizations (ISAOs).” Accessed April 9, 2016. https://www.dhs.gov/isao.

———. *Memorandum of Agreement between the Department of Homeland Security and The Department of Defense Regarding Cybersecurity*. Washington, DC: Department of Homeland Security, 2010. http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf.

———. “National Network of Fusion Centers Fact Sheet.” Accessed January 15, 2014. https://www.dhs.gov/national-network-fusion-centers-fact-sheet#1.

———. *National Preparedness Report.* Washington, DC: Department of Homeland Security, 2012. http://www.fema.gov/media-library-data/20130726-1833-25045-2705/national_preparedness_report_20120330_v2_1.pdf.

———. “Remarks by Secretary Napolitano at the Council on Foreign Relations.” July 29, 2009. http://www.dhs.gov/ynews/speeches/sp_1248891649195.shtm.

———. “Secure Cyber Networks.” Accessed January 31, 2014. https://www.dhs.gov/secure-cyber-networks.

———. “State and Major Urban Area Fusion Centers.” Accessed February 11, 2014. http://www.dhs.gov/state-and-major-urban-area-fusion-centers.

———. “State, Local, Tribal, and Territorial Government Coordinating Council: Charter and Membership.” April 13, 2016. https://www.dhs.gov/slttgcc-charter-and-membership.

Diamondback, The. “University of Maryland Researchers Fend off Steady Cyber Risks.” Accessed January 17, 2014. http://www.diamondbackonline.com/news/campus/article_4158cd62-fa5c-11e2-afd7-0019bb30f31a.html.

Dictionary.com. “Cyberterrorism.” Accessed February 18, 2016. http://dictionary.reference.com/browse/cyberterrorism?s=t.

Digital Attack Map. “Digital Attack Map.” Accessed February 12, 2015. http://www.digitalattackmap.com/understanding-ddos/.

Duanesburg, New York. “Duanesburg Central School District.” Accessed January 15, 2013. http://duanesburg.org/district/news/0910/overview_onlinetheft.cfm.

FBI. “Charges Unsealed against Five Alleged Members of Al Qaeda Plot to Attack the United States and the United Kingdom.” Accessed November 1, 2013. http://www.fbi.gov/newyork/press-releases/2010/nyfo070710a.htm.

———. “Five Chinese Military Hackers Charged with Cyber Espionage against U.S..” Accessed February 12, 2015. http://www.fbi.gov/news/news_blog/five-chinese-military-hackers-charged-with-cyber-espionage-against-u.s.

FCW. “DHS, Industry to Try Fusion Centers for Classified Data Swap.” Accessed February 11, 2014. http://fcw.com/Articles/2010/03/16/Web-cyber-threat-fusion-center.aspx?p=1.

Federal Register. “Improving Critical Infrastructure Cybersecurity.” Accessed February 1, 2014. https://www.federalregister.gov/articles/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity.

FederalNewsRadio.com. “OPM Notifies 3.7 Million Cyber Attack Victims.” October 28, 2015. http://federalnewsradio.com/cybersecurity/2015/10/opm-notifies-3-7-million-cyber-attack-victims-about-data-protection-services/.

FEMA. *2012 National Preparedness Report (NPR)*. Washington, DC: FEMA, 2012.

———. *National Preparedness Report*. Washington, DC: FEMA, 2015. http://www.fema.gov/national-preparedness-report.

FireEye, Center for Digital Government. “Advanced Cyber Threats in State and Local Government.” 2. Accessed February 1, 2015. http://images.erepublic.com/documents/CDG14+SURVEY+FireEye_V2.pdf.

Goldman, David. “Cyberattacks on Critical U.S. Infrastructure Rose 52% in 2012.” *CNNMoney*, January 9, 2013. http://money.cnn.com/2013/01/09/technology/security/infrastructure-cyberattacks/index.html.

Gongwer. “New State Budget Would Give $5 Million Boost to State Cybersecurity Protection.” February 11, 2016, Mitechnews.Com. http://mitechnews.com/politics/new-state-budget-would-give-5-million-boost-to-state-cybersecurity-protection/.

Gorman, Siobhan. “Iran Renews Internet Attacks on U.S. Banks.” *Wall Street Journal*, October 18, 2012, sec. Tech. http://www.wsj.com/articles/SB10000872396390444592704578063063201649282.

Government Technology. “Washington State Courts Office Suffers Data Breach.” May 9, 2013. http://www.govtech.com/security/Washington-State-Courts-Suffers-Data-Breach.html.

Grandoni, Dino. “The Most Destructive Virus to Ever Hit a Business?.” *The Huffington Post*. Accessed February 18, 2016. http://www.huffingtonpost.com/2012/10/11/shamoon-virus-leon-panetta_n_1960113.html.

Great Dreams. “Regional Contacts.” Accessed April 8, 2013. http://www.greatdreams.com/political/RegionalContacts.jpg.

Harrington, Elizabeth. “Expert: Healthcare.gov Security Risks Even Worse After ‘Fix.’” *Washington Free Beacon*. Accessed January 21, 2014. http://freebeacon.com/expert-healthcare-gov-security-risks-even-worse-after-fix/.

Harris, Barry. “Stabilizing Iraq: Intelligence Lessons for Afghanistan.” The Washington Institute, May 29, 2009. http://www.washingtoninstitute.org/policy-analysis/view/stabilizing-iraq-intelligence-lessons-for-afghanistan.

Heartbleed.com. “Heartbleed Bug.” Accessed February 10, 2015. http://heartbleed.com/.

Heaton, Brian. “New Jersey’s Cyber Fusion Cell Collaborates on Cyberthreats.” Emergency Management, September 23, 2013. http://www.emergencymgmt.com/safety/New-Jerseys-Cyber-Fusion-Cell.html.

Hewlett Packard. “State of Cybersecurity in Government FINAL.” Accessed March 3, 2016. https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6-2563enw.pdf.

Homeland Security News Wire. “Cybersecurity: Police Department Pays Ransom after Hackers Encrypt Department’s Data.” April 6, 2015. http://www.homelandsecuritynewswire.com/dr20150406-police-department-pays-ransom-after-hackers-encrypt-department-s-data.

Information Sharing Environment. “Fusion Centers and Private Sector Come Together on Cybersecurity.” Accessed January 15, 2014. https://www.ise.gov/blog/mike-sena/fusion-centers-and-private-sector-come-together-cybersecurity.

———. “Fusion Centers and Public-Private Collaboration.” Accessed February 17, 2014. http://ise.gov/blog/major-thomas-souchek/fusion-centers-and-public-private-collaboration.

Information Technology Sector. “Specific Plan 201.” Accessed February 11, 2014. http://www.it-scc.org/documents/itscc/nipp-ssp-information-tech-2010.pdf.

Infosecurity. “DHS Teams with DOD on Cybersecurity Project with Industry.” Accessed January 31, 2014. http://www.infosecurity-magazine.com/view/23348/dhs-teams-with-dod-on-cybersecurity-project-with-industry/.

Infragard Members Alliance Louisiana. “DHS_CSA_Cyber_Brief_AMSC_20140123_Willke.pdf.” Accessed March 10, 2016. http://infragardlouisiana.com/wp-content/uploads/2015/10/DHS_CSA_Cyber_Brief_AMSC_20140123_Willke.pdf.

Isikoff, Michael. “HealthCare.gov Targeted ‘about 16 Times’ by Cyberattacks, DHS Official Says.” *NBC News*, November 13, 2013. http://investigations.nbcnews.com/_news/2013/11/13/21440068-healthcaregov-targeted-about-16-times-by-cyberattacks-dhs-official-says.

———. “One Email Exposes Millions of Personal Data Theft in South Carolina Cyber Attack.” *NBC News*, November 20, 2012. http://investigations.nbcnews.com/_news/2012/11/20/15313720-one-email-exposes-millions-of-people-to-data-theft-in-south-carolina-cyberattack.

IT Sector Coordinating Council. “ITSCC Overview.” Accessed March 17, 2014. http://www.it-scc.org/about.html.

Kramer, Franklin D. *Policy Recommendations for a Strategic Framework*. Washington, DC: Cyberpower and National Security, National Defense University Press, 2010.

KSL.com. “State Faces Millions of Cyber Attacks per Day, Department Head Says.” Accessed March 6, 2015. http://www.ksl.com/?nid=148&sid=24141005.

Lipman, Paul. “4 Critical Challenges to State and Local Government Cybersecurity Efforts (Industry Perspective).” Government Technology, July 17, 2015. http://www.govtech.com/opinion/4-Critical-Challenges-to-State-and-Local-Government-Cybersecurity-Efforts.html.

Lyngaas, Sean. “Cyber Threat Challenges Military Structure.” The Business of Federal Technology, February 23, 2015. https://fcw.com/articles/2015/02/23/cyber-threat-challenges-military.aspx.

McAfee. “Protecting Yourself from the Conficker Worm.” Accessed February 12, 2015. http://home.mcafee.com/root/landingpage.aspx?affid=0&lpname=18310&cid=54857&culture=en-US&legacylangcd=en-us.

McCaney, Kevin. “Got a Cyber Emergency? Call out the National Guard.” Defense Systems, January 30, 2014. http://defensesystems.com/articles/2014/01/30/national-guard-cyber-response.aspx.

McCarter, Mickey. “Senators Seek National Guard Cybersecurity Civil Support Teams.” Homeland Security Today, March 27, 2013. http://www.hstoday.us/briefings/daily-news-analysis/single-article/senators-seek-national-guard-cybersecurity-civil-support-teams/8461dd77befa9b1506273a976c5c2b15.html.

———. “U.S. National Guard: Senators Seek National Guard Cybersecurity Civil Support Teams.” Homeland Security Today, March 27, 2013. http://www.hstoday.us/channels/us-national-guard/single-article-page/senators-seek-national-guard-cybersecurity-civil-support-teams/8461dd77befa9b1506273a976c5c2b15.html.

Michigan Cyber Civilian Corps. “About MiC3.” Accessed March 11, 2016. http://www.micybercorps.org/about.php.

mile2. “Information Assurance Philosophy—Green Hat, Cyber Security and Information Assurance.” https://www.mile2.com/ia-philosophy.html?tmpl=component&print=1&page=.

Multi-State Information Sharing & Analysis Center. *MS-ISAC Membership Overview*. East Greenbush, NY: Center for Internet Security, 2012. http://msisac.cisecurity.org/about/documents/MS-ISACMembershipOverview2012.pdf.

Murray, Teresa. “KeyCorp, U.S. Bank Websites Hit in the Latest Cyber Attack against Nation’s Largest Banks.” Cleveland.com. September 12, 2012. http://www.cleveland.com/business/index.ssf/2012/09/keycorp_us_bank_web_sites_hit.html.

Napolitano, Janet. “Cyber Attacks One of the Most Serious Threats.” Infosecurity. September 11, 2012, www.Infosecurity-Magazine.com.

———. “U.S. Homeland Chief: Cyber 9/11 Could Happen “Imminently.”“ Reuters. January 24, 2013, www.Reuters.com/article.

Nasr, Amir. “Universities Increasingly Falling Victim to Cyberattacks.” *Morning Consult*, July 11, 2015. http://morningconsult.com/2015/07/universities-increasingly-falling-victim-to-cyberattacks/.

National Association State Chief Information Officers. “State IT Workforce: Facing Reality with Innovation.” April 2015. http://www.nascio.org/Publications/ArtMID/485/ArticleID/79/State-IT-Workforce-Facing-Reality-with-Innovation.

National Association of State Chief Information Officers (NASCIO). *2012 Deloitte-NASCIO Cybersecurity Study, State Governments at Risk: A Call for Collaboration and Compliance*. Lexington, KY: National Association of State Chief Information Officers NASCIO, 2012. http://www.nascio.org/Surveys/ArtMID/557/ArticleID/106/2012-Deloitte-NASCIO-Cybersecurity-Study-State-governments-at-Risk-A-Call-for-Collaboration-and-Compliance.

National Commission on Terrorist Attacks Upon the United States, The. *The 9/11 Commission Report*. Washington, DC: National Commission on Terrorist Attacks Upon the United States, 2004. http://govinfo.library.unt.edu/911/report/911Report_Ch13.pdf.

National Cybersecurity and Communications Integration Center. *ICS-CERT Year in Review*. Washington, DC: Department of Homeland Security, 2013. https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_In_Review_FY2013_Final.pdf.

National Governors Association. “Cybersecurity Workforce Key to Combating Threats.” Accessed April 22, 2016. http://www.nga.org/cms/home/news-room/news-releases/2014--news-releases/col2-content/cybersecurity-workforce-key-to-c.html.

National Infrastructure Advisory Council. *Intelligence Information Sharing, Final Report and Recommendations*. Washington, DC: Department of Homeland Security, 2012. http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf.

Naval Postgraduate School, Center for Homeland Defense & Security. “Fusion Centers Are Meeting Shifting Security Challenges.” June 29, 2012. https://www.chds.us/c/item/771.

Netcraft, “Half a Million Widely Trusted websites Vulnerable to Heartbleed Bug.” Accessed February 10, 2015. http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html.

Networkworld. “DHS: America’s Water and Power Utilities under Daily Cyber-Attack, April 4, 2012. http://www.networkworld.com/news/2012/040412-dhs-cyberattack-257946.html.

New York Times, The. “Worm Infects Millions of Computers Worldwide.” Accessed March 14, 2014. http://www.nytimes.com/2009/01/23/technology/internet/23worm.html?_r=0.

Nextgov, “Is There Any Part of Government That Hasn’t Been Hacked Yet?.” Accessed February 19, 2016. http://www.nextgov.com/cybersecurity/2014/09/there-any-part-government -hasnt-been-hacked-yet/93704/.

NextGov.com. “Defense and DHS Reach Cybersecurity Compromise.” Accessed January 31, 2014. http://www.nextgov.com/cybersecurity/2010/10/defense-and-dhs-reach-cybersecurity-compromise/47758/.

NSA/CSS. “National Centers of Academic Excellence in Information Assurance (IA)/Cyber Defense (CD).” Accessed April 12, 2016. https://www.nsa.gov/ia/academic_outreach/nat_cae/.

Office of Cybersecurity and Communications. *CSA Security Advisor Initiative Pre-Decisional Implementation Plan*. Washington, DC: Department of Homeland Security, 2014.

Office of Justice Programs, Bureau of Justice Assistance. *Fusion Center Guidelines Developing and Sharing Information and Intelligence in a New Era*. Washington, DC: Department of Justice, 2006. https://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf.

PCTools. “What Is a Computer Worm.” Accessed February 12, 2015. http://www.pctools.com/security-news/what-is-a-computer-worm/.

PCWorld, “Adobe Pushes Critical Flash Player Update to Fix Latest Zero-Day.” January 26, 2015. http://www.pcworld.com/article/2875252/adobe-pushes-critical-flash-player-update-to-fix-latest-zeroday.html.

Pellerin, Cheryl. “Cybersecurity Involves Federal, Industry Partners, Allies, American Forces Press Service.” Department of Defense. Accessed December 15, 2012. http://archive.defense.gov/news/newsarticle.aspx?id=118479.

Pérez-peña, Richard. “Universities Face a Rising Barrage of Cyberattacks.” *The New York Times*, July 16, 2013. http://www.nytimes.com/2013/07/17/education/barrage-of-cyberattacks-challenges-campus-culture.html.

Perlroth, Nicole, and Quentin Hardy. “Online Banking Attacks Were Work of Iran, U.S. Officials Say.” *The New York Times*, January 8, 2013. http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html.

Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs. *Federal Support for and Involvement in State and Local Fusion Centers Majority and Minority Staff Report Permanent Subcommittee on Investigations United States Senate*. Washington, DC: United States Senate, 2012. http://cdn.govexec.com/media/gbc/docs/pdfs_edit/100312cc1.pdf.

Pew Charitable Trusts State and Consumer Initiatives Site Map Search, The. “The National Guard Takes on Hackers.” *The Pew Charitable Trusts*, January 28, 2014. http://www.pewstates.org/projects/stateline/headlines/the-national-guard-takes-on-hackers-85899535957.

Poeter, Damon. “50 Days of Mayhem: How LulzSec Changed Hacktivism Forever.” PCMag.com. Accessed March 3, 2016. http://www.pcmag.com/article2/0,2817,2387716,00.asp.

Ponemon Institute. “The State of Cybersecurity in Local, State and Federal Government.” October 9, 2015. http://www.ponemon.org/blog/the-state-of-cybersecurity-in-local-state-and-federal-government.

———. *2011 Cost of Data Breach Study: Global*. Traverse City, MI: Ponemon Institute, 2012.

Privacy and Security Law Blog. “Executive Order and Policy Directive Promotes Cybersecurity Cooperation and Intelligence Sharing.” Accessed February 1, 2014. http://www.privsecblog.com/2013/02/articles/main-topics/data-breach-security/executive-order-and-policy-directive-promotes-cybersecurity-cooperation-and-intelligence-sharing/.

Rapid7. *Data Breaches in the Government Sector*. Boston, MA: Rapid7, 2012.

Ratman, Gopal. “Cyberattacks Could Become as Destructive as 9/11: Panetta.” Bloomberg, October 11, 2012. http://www.bloomberg.com/news/articles/2012-10-12/cyberattacks-could-become-as-destructive-as-9-11-panetta.

Reagor, Todd. “DDOS Attacks on Chase Point to Iran Hacker Group.” *Rivalhost Blog*, September 21, 2012. https://www.rivalhost.com/blog/ddos-attacks-on-chase-point-to-iran-hacker-group/.

Reitinger, Philip. *Enabling Distributed Security in Cyberspace, Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action, Department of Homeland Security*. Washington, DC: Department of Homeland Security, 2011. https://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf.

Rollins, John. *Fusion Centers: Issues and Options for Congress* (CRS Report No. RL34070). Washington, DC: Congressional Research Service, 2008. https://www.fas.org/sgp/crs/intel/RL34070.pdf.

Security Affairs. "Verizon Report, the Wind of Hacktivism Pushes Cybercrime." March 22, 2012. http://securityaffairs.co/wordpress/3524/cyber-crime/verizon-report-the-wind-of-hacktivism-pushes-cybercrime.html.

Serrao, Stephen. "Fusion Centers: Defining Success." Homeland Security Today, October 13, 2009. http://www.hstoday.us/blogs/best-practices/blog/fusion-centers-defining-success/d2adf8a8025faecbe0268d81fe1d3c54.html.

Simonite, Tom. "Old-Fashioned Control Systems Make U.S. Power Grids, Water Plants a Hacking Target." Security, October 12, 2012. http://securitynewsworld.wordpress.com/2012/10/15/old-fashioned-control-systems-make-u-s-power-grids-water-plants-a-hacking-target/.

Spidalieri, Francesca. *State of the States on Cybersecurity*. Newport, RI: Pell Center, 2015. http://pellcenter.org/wp-content/uploads/2015/11/Pell-Center-State-of-the-States-Report.pdf.

StateScoop Staff. "New York Cyber Fusion Center to Relocate to CIS." *StateScoop*. Accessed March 15, 2016. http://statescoop.com/new-york-cyber-fusion-center-relocate-cis.

Symantec Security Response. "ShellShock: All You Need to Know about the Bash Bug Vulnerability." Accessed February 10, 2015. http://www.symantec.com/connect/blogs/shellshock-all-you-need-know-about-bash-bug-vulnerability.

———. "The Shamoon Attacks." Accessed February 18, 2016. http://www.symantec.com/connect/blogs/shamoon-attacks.

Symantec. "Psychology Behind Intellectual Property Theft by Corporate Insiders." Accessed 14 October 2012. https://www.symantec.com/about/newsroom/press-releases/2011/symantec_1207_01.

U.S. Government Accountability Office. "About GAO." Accessed March 6, 2015. http://www.gao.gov/about/index.html.

———. *Cybersecurity: A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges Statement of Gregory C. Wilshusen, Director Information Security Issues*. (GAO-13-462T). Washington, DC: U.S. Government Accountability Office, 2013. http://www.gao.gov/products/GAO-13-462T.

———. *Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure Statement of Gregory C. Wilshusen, Director, Information Security Issues*/. (GAO-11-865T). Washington, DC: U.S. Government Accountability Office, 2011. http://www.gao.gov/assets/130/126702.pdf.

———. *Cybersecurity: Threats Impacting the Nation, Statement of Gregory C. Wilshusen, Director, Information Security Issues*. (GAO-12-666T). Washington, DC: U.S. Government Accountability Office, 2012. http://www.gao.gov/assets/600/590367.pdf.

———. *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent*. (GAO-14-34). Washington, DC: U.S. Government Accountability Office, 2013. http://www.gao.gov/assets/660/659572.pdf.

———. *Protecting Personally Identifiable Information*. (GAO-08-343). Washington, DC: U.S. Government Accountability Office, 2008. http://www.gao.gov/new.items/d08343.pdf

United States Senate. *Permanent Subcommittee on Investigations, Federal Support for and Involvement in State and Local Fusion Centers*. Washington, DC: United States Senate, 2012. www.CDN.GOVEXEC.com.

UPI. "U.S. Officials Say What's Been Stolen in Cyberattacks Sometimes Not Known." July 17, 2013. http://www.upi.com/Top_News/US/2013/07/17/US-research-universities-increasingly-targeted-by-cyberattacks/UPI-26641374065244/.

USA Today. "Timeline: North Korea and the Sony Pictures Hack." Accessed February 12, 2015. http://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/.

———. "Why the Shamoon Virus Looms as Destructive Threat." Accessed February 18, 2016. http://www.usatoday.com/story/cybertruth/2013/05/16/shamoon-cyber-warfare-hackers-anti-american/2166147/.

Wall Street Journal, The. "Booz Allen Says Cyber Attacks Are the 'New Normal' for Financial Services Industry." Accessed March 3, 2014. http://online.wsj.com/article/PR-CO-20131204-908341.html.

White House, The. *Cyberspace Policy Review, Assuring a Trusted and Resilient Information and Communication Infrastructure*. Washington, DC: The White House, 2009. https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

———. "Executive Order—Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities." Accessed April 15, 2015. https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m.

———. "Executive Order—Promoting Private Sector Cybersecurity Information Sharing." Accessed March 21, 2015. https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari.

———. "National Cybersecurity Center Policy Capture." Accessed December 12, 2012. http://www.whitehouse.gov/files/documents/cyber/CybersecurityCentersGraphic.pdf.

———. *National Security Strategy*. Washington, DC: The White House, 2010. http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

———. "President Obama on Cybersecurity." Transcript, The White House, May 29, 2009.

———. "Presidential Policy Directive—Critical Infrastructure Security and Resilience." Accessed March 6, 2015. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

———. *Presidential Policy Directive/PPD-21*. Washington, DC: The White House, 2013.

———. "The Comprehensive National Cybersecurity Initiative." Accessed March 4, 2014. http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative.

Wood, Colin. "L.A.'s Cyber Intrusion Command Center: A Model for Cybersecurity Governance?." Emergency Management, May 27, 2104. http://www.emergencymgmt.com/safety/LAs-Cyber-Intrusion-Command-Center-Cybersecurity.html.

Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapon." *WIRED*, November 3, 2014. http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California